MAKE THE
WORLD SEE

Milestone Systems

XProtect® VMS 2018 R2

Manual del administrador

XProtect Corporate

XProtect Expert

XProtect Professional+

XProtect Express+

XProtect Essential+

Este texto ha sido traducido de forma automática.

milestone

Contenido

Copyright, marcas comerciales y limitación de responsabilidad

Marcas comerciales

XProtect es una marca comercial registrada de Milestone Systems A/S.

Microsoft y Windows son marcas registradas de Microsoft Corporation. App Store es una marca de servicio de Apple Inc. Android es una marca comercial de Google Inc.

Todas las demás marcas comerciales de este documento pertenecen a sus respectivos propietarios.

Limitación de responsabilidad

Este documento está únicamente concebido como información general, y se ha elaborado con la debida diligencia.

Cualquier daño que pueda derivarse del uso de esta información será responsabilidad del destinatario, y nada de lo aquí escrito podrá ser considerado como ningún tipo de garantía.

Milestone Systems A/S se reserva el derecho a hacer modificaciones sin notificación previa.

Todos los nombres de personas y organizaciones utilizados en los ejemplos de este documento son ficticios. Cualquier parecido con una organización o persona reales, viva o muerta, es pura coincidencia y carece de intencionalidad alguna.

Este producto puede hacer uso de un software de terceros al que es posible que se apliquen términos y condiciones específicas. Si ese es el caso, puede encontrar más información en el archivo 3rd_party_software_terms_and_conditions.txt que se encuentra en la carpeta de instalación del sistema de vigilancia de Milestone.

Antes de empezar

Introducción a este manual

Este manual cubre los siguientes productos:

- XProtect Corporate
- XProtect Expert
- XProtect Professional+
- XProtect Express+
- XProtect Essential+

La documentación describe todos los ajustes y funcionalidades disponibles cuando utiliza el producto más rico en funciones, XProtect Corporate.

Si está utilizando uno de los otros productos, tiene menos funcionalidad disponible para usted. Los temas pueden mencionar funcionalidades o configuraciones que sólo están disponibles en un producto más avanzado. En estos casos, las notas en la parte superior de la sección correspondiente indican que es posible que no disponga de esta funcionalidad.

Para obtener más información sobre la funcionalidad disponible en su sistema, consulte el gráfico de comparación de productos (ver "Tabla de comparación de productos" en la página 24).

Estructura de la ayuda

La ayuda se divide en secciones que cada una tiene un propósito específico. Las secciones se estructuran en un flujo lógico:

Sección	Descripción
Información general del sistema (en la página 16)	Proporciona una introducción a su sistema de video vigilancia, los componentes del sistema, y los conceptos. Esto es útil si usted es nuevo en el sistema. La visión general del sistema también proporciona una tabla de comparación que muestra las diferencias más significativas entre los productos.
Instalación (en la página 30)	Proporciona condiciones de instalación y los procedimientos paso a paso para ayudarle a instalar y actualizar el sistema.
Primer uso (en la página 62)	Proporciona una visión general del Management Client e información sobre las mejores prácticas a seguir para que el sistema funcione a la perfección. Esta visión general es útil si usted es nuevo en el sistema.
Elementos Management Client (en la página 71)	Proporciona un recorrido exhaustivo de cada uno de los nodos en el panel **Navegación del sitio** del Management Client. Esta sección contiene información conceptual e instrucciones para los elementos básicos de su sistema.

Sección	Descripción
Configuración de funciones (en la página 293)	Proporciona en sí misma, la información detallada sobre las características adicionales y los productos complementarios de los que da soporte el sistema.
Mantenimiento del sistema (en la página 442)	Proporciona una visión general de los puertos utilizados en el sistema y los procedimientos paso a paso para, por ejemplo, copias de seguridad del sistema y la supervisión del rendimiento del sistema. Esta sección es útil después de la instalación y la configuración con el fin de mantener, ampliar y optimizar su sistema.

Navegación por el sistema de ayuda integrado

Pulse F1 para acceder a un tema de ayuda relacionado o seleccione **Ayuda** > **Contenido** de la barra de herramientas Management Client para iniciar la ayuda completa.

Puede navegar entre las tres pestañas de la ventana de ayuda: **Contenido**, **Índice**, y la **búsqueda** o utilice los enlaces dentro de los temas de ayuda.

Pestaña	Descripción
Contenido	Navegue por el sistema de ayuda mediante una estructura de árbol.
Índice	Seleccione la primera letra de la palabra que usted está interesado y desplazarse hasta que lo encuentres. Haga clic en un título de tema de ayuda en la lista de resultados de búsqueda para abrir el tema requerido.
Buscar	Buscar temas de ayuda que contengan términos particulares de interés. Por ejemplo, busque el término **zoom** y reciba una lista en el resultado de la búsqueda de todos los temas de ayuda que contengan el término **zoom**. Haga clic en un título de tema de ayuda en la lista de resultados de búsqueda para abrir el tema requerido.

Para imprimir un tema de ayuda, vaya al tema deseado y haga clic en el botón **Print (imprimir)** del navegador.

Información general del sistema

Descripción del producto

Los productos VMS de XProtect son software de gestión de vídeo diseñado para instalaciones de todas las formas y tamaños. Si desea proteger su tienda contra el vandalismo o desea administrar una instalación multi-sitio de alta seguridad, XProtect lo hace posible. Las soluciones ofrecen una gestión centralizada de todos los dispositivos, servidores y usuarios, y proporcionan un sistema de reglas extremadamente flexible basado en horarios y eventos.

Su sistema consta de los siguientes elementos principales:

- El servidor de gestión - el centro de la instalación, consta de varios servidores.
- Uno o más **servidores de grabación** .
- Uno o más **XProtect Management Client s** .
- **XProtect Download Manager**.
- Uno o más **XProtect® Smart Client s** .
- Uno o más **XProtect Web Client** y / o **clientes Milestone Mobile** si es necesario.

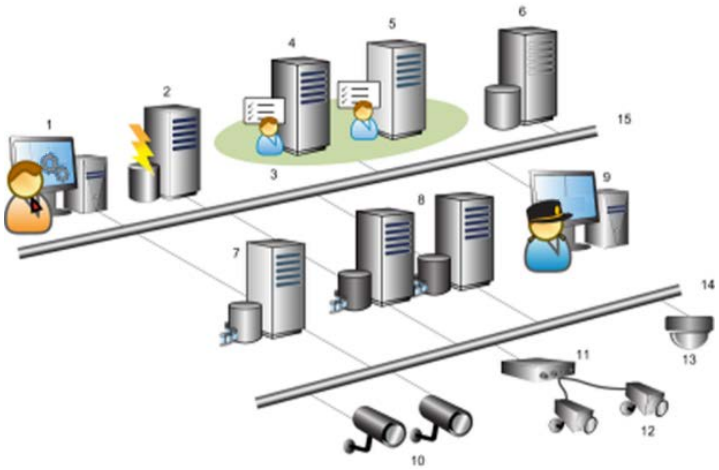
Su sistema también incluye una funcionalidad totalmente integrada de Matrix para la visualización distribuida de vídeo desde cualquier cámara de su sistema de vigilancia a cualquier computadora con XProtect Smart Client instalada.

Puede instalar su sistema en servidores virtualizados o en varios servidores físicos en una instalación distribuida.

El sistema también ofrece la posibilidad de incluir el XProtect® Smart Client – Player independiente al exportar evidencia de vídeo desde el XProtect Smart Client. XProtect Smart Client – Player permite a los destinatarios de pruebas de vídeo (como policías, investigadores internos o externos y más) navegar y reproducir las grabaciones exportadas sin tener que instalar ningún software en sus computadoras.

Con los productos más ricos en características instalados (ver "Tabla de comparación de productos" en la página 24) su sistema puede manejar un número ilimitado de cámaras, servidores y usuarios ya través de múltiples sitios si es necesario. Su sistema puede manejar IPv4 así como IPv6.

Una configuración de sistema distribuida



Ejemplo de configuración del sistema. El número de cámaras, servidores de grabación, y los clientes conectados, puede ser tan alto como sea necesario.

Leyenda:

1. Management Client(s)
2. Servidor de eventos
3. Clúster de Microsoft
4. Servidor de gestión
5. Servidor de gestión failover
6. Servidor SQL
7. Servidor de grabación failover
8. Servidor(es) de grabación
9. XProtect Smart Client(s)
10. Cámaras de vídeo IP
11. Servidor de vídeo
12. Cámaras analógicas
13. Cámara PTZ IP
14. Red de cámaras
15. Red del servidor

Componentes del sistema

Servidor de gestión

El servidor de gestión es el componente central del sistema VMS. Almacena la configuración del sistema de vigilancia en una base de datos relacional, ya sea en el equipo servidor de gestión en sí o en un servidor SQL independiente en la red. También maneja la autenticación de usuarios, derechos de usuario, el sistema de reglas y más. Para mejorar el rendimiento del sistema, puede ejecutar varios servidores de administración como Milestone Federated Architecture™. El servidor de gestión se ejecuta como un servicio, y por lo general se instala en un servidor dedicado.

Los usuarios se conectan al servidor de gestión para la autenticación inicial, a continuación, de forma transparente para los servidores de grabación para el acceso a las grabaciones de vídeo, etc.

Servidor de gestión failover

El soporte de conmutación por error en el servidor de administración se logra instalando el servidor de administración en un clúster de Microsoft Windows. El clúster se asegurará de que el nuevo servidor sustituto se haga cargo de la función del servidor de administración en caso que falle el primer servidor.

Servidor de grabación

El servidor de grabación es responsable de la comunicación con las cámaras de red y codificadores de vídeo, grabación de audio y vídeo recuperada, así como proporcionar acceso de clientes a en vivo y grabados de audio y vídeo. El servidor de grabación también es responsable de la comunicación con otros productos de Milestone conectados a través de la tecnología de Milestone Interconnect.

Controladores de dispositivos

- La comunicación con las cámaras de red y los codificadores de video se realiza a través de un controlador de dispositivo desarrollado específicamente para dispositivos individuales o una serie de dispositivos similares de la misma fabricación.
- A partir de la versión 2018 R1, los controladores del dispositivo se dividen en dos paquetes de dispositivos: el paquete de dispositivo regular con controladores más nuevos y un paquete de dispositivo heredado con controladores más antiguos.
- El paquete de dispositivo regular se instala automáticamente cuando instala el servidor de grabación. Más tarde, puede actualizar los controladores descargando e instalando una versión más nueva del paquete de dispositivo.
- El paquete de dispositivo heredado solo se puede instalar si el sistema tiene un paquete de dispositivo normal instalado. Los controladores del paquete de dispositivo heredado se instalan automáticamente si ya hay una versión anterior instalada en su sistema. Está disponible para descarga e instalación manual en la página de descarga de software (http://www.milestonesys.com/downloads).

Base de datos de medios

- Los datos de audio y de vídeo recuperada se almacena en la base de datos de medios de comunicación de alto rendimiento a medida optimizado para el grabación y almacenamiento de datos de audio y de vídeo.

- La base de datos de medios de comunicación admite varias características únicas como; Archivo de múltiples etapas, video grooming, cifrado, y añadir una firma digital a las grabaciones.

Servidor de grabación failover

El servidor de grabación de conmutación por error es responsable de asumir la tarea de grabación si falla un servidor de grabación.

El servidor de grabación failover puede funcionar en dos modos:

- Cold standby - para supervisar múltiples servidores de grabación
- Hot standby - para supervisar un único servidor de grabación

La diferencia entre los modos de espera en frío y en caliente es que en el modo de espera en frío, el servidor de grabación de conmutación por error no sabe de qué servidor se hará cargo, por lo que no puede iniciarse hasta que falla un servidor de grabación. En el modo de espera en caliente, el tiempo de conmutación por error es significativamente más corto, ya que el servidor de grabación de conmutación por error ya sabe qué servidor de grabación debe tomar el relevo y puede precargar la configuración y arrancar completamente, excepto el último paso de conexión a las cámaras.

Servidor Mobile

El servidor Mobile es responsable de permitir que los usuarios Milestone Mobile y XProtect Web Client accedan al sistema.

Además de actuar como una pasarela de sistema para los dos clientes, el servidor Mobile puede transcodificar vídeo, ya que en muchos casos la secuencia de vídeo original de la cámara es demasiado grande para ajustar el ancho de banda disponible para los usuarios del cliente.

Si está realizando una instalación **Distribuido** o **Personalizada**, Milestone recomienda instalar el servidor Mobile en un servidor dedicado.

Servidor de eventos

El servidor de eventos gestiona varias tareas relacionadas con eventos, alarmas, mapas y integraciones de terceros a través del kit de desarrollo de software MIP (SDK).

Eventos:

- Todos los eventos del sistema se consolidan en el servidor de eventos por lo que hay un solo lugar y la interfaz de socios para realizar integraciones que utilizan los eventos del sistema.
- Además, el servidor de eventos ofrece 3ª acceso de terceros a enviar eventos al sistema a través de los eventos genéricos o interfaz de Evento de Analytics.

Alarmas:

- El servidor de eventos acoge la función de alarma, la lógica de alarma, estado de alarma, así como el manejo de la base de datos de alarma. La base de datos de alarma se almacena en el mismo servidor SQL utiliza el servidor de gestión.

Mapas:

- El servidor de eventos también alberga los mapas que están configurados y utilizados en XProtect Smart Client.

MIP SDK:

- Por último, terceros-desarrollado plug-ins se pueden instalar en el servidor de eventos y utilizar el acceso a los eventos del sistema.

Servidor de registro

El servidor de registro se encarga de almacenar todos los mensajes de registro para todo el sistema. El servidor de registro utiliza el mismo servidor SQL como el servidor de gestión y típicamente está instalado en el mismo servidor que el servidor de gestión, pero se puede instalar en un servidor independiente si es necesario para aumentar el rendimiento de los servidores de gestión y registro.

SQL server

El servidor de gestión, el servidor de eventos y el servidor de registro utilizan un servidor SQL para almacenar, por ejemplo, la configuración, las alarmas, los eventos y los mensajes de registro.

El instalador del sistema incluye Microsoft SQL Server Express que se puede utilizar libremente para sistemas de hasta 300 cámaras.

Para sistemas grandes de más de 300 cámaras, Milestone recomienda que use un servidor SQL dedicado con, por ejemplo, Microsoft SQL Server Standard instalado ya que esta edición puede manejar bases de datos más grandes y ofrece funcionalidad de respaldo.

Active Directory

Active Directory es un servicio de directorio distribuido Implementado por Microsoft para Dominio de Windows redes. Se incluye en la mayoría de los sistemas operativos Windows Server. Identifica recursos de una red para que los usuarios o las aplicaciones puedan acceder a ellos.

Con el Active Directory instalado, puede añadir usuarios de Windows de Active Directory, pero también tiene la opción de añadir usuarios básicos sin Active Directory. Tenga en cuenta que hay ciertas limitaciones del sistema relacionados con los usuarios básicos.

Servidores virtuales

Puede ejecutar todos los componentes del sistema en Windows virtualizado ® servidores, tales como VMware® y Microsoft® Hyper-V®.

La virtualización es a menudo preferido para utilizar mejor los recursos de hardware. Normalmente, los servidores virtuales que se ejecutan en el servidor host de hardware no se cargan en el servidor virtual, en gran medida, y con frecuencia no al mismo tiempo. Sin embargo, los servidores de grabación de grabar todas las cámaras y las secuencias de vídeo. Esto pone a la alta carga de CPU, memoria, red y sistema de almacenamiento. Por lo tanto, cuando se ejecuta en un servidor virtual, la ganancia normal de virtualización desaparece en gran medida, ya que - en muchos casos - que utiliza todos los recursos disponibles.

Si se ejecuta en un entorno virtual, es importante que el anfitrión de hardware tiene la misma cantidad de memoria física que asigna a los servidores virtuales y que el servidor virtual que se ejecuta el servidor de grabación se asigna suficiente CPU y la memoria - que no lo es por defecto. Por lo general, el servidor de registro de necesidades 2-4 GB dependiendo de la configuración. Otro cuello de botella es la asignación de adaptador de red y el rendimiento del disco duro. Considerar la asignación de un adaptador de red físico en el servidor host del servidor virtual que se ejecuta el servidor de grabación. Esto hace que sea más fácil para asegurar que el adaptador de red no está sobrecargado con el tráfico a otros servidores virtuales. Si se utiliza el adaptador de red para distintos servidores virtuales, el tráfico de la red puede hacer que el servidor de grabación no reciba y grabe la cantidad de imágenes establecida.

Clientes

Management Client (explicado)

Cliente de administración rico en funciones para la configuración y gestión diaria del sistema. Disponible en varios idiomas.

Suele instalarse en la estación de trabajo del administrador del sistema de vigilancia o similar.

Para una descripción detallada del Management Client, vea Introducción a la Management Client (ver "Resumen de Management Client" en la página 64).

XProtect Smart Client (explicado)

Diseñado para Milestone XProtect® Software de gestión de vídeo IP, el XProtect Smart Client es una aplicación cliente fácil de usar que proporciona un control intuitivo sobre las instalaciones de seguridad. Manejo de las instalaciones de seguridad con XProtect Smart Client que da a los usuarios acceso a vídeo en directo y grabado, control instantáneo de las cámaras y los dispositivos de seguridad conectados, y una visión general de las grabaciones. Disponible en varios idiomas locales, XProtect Smart Client tiene una interfaz de usuario adaptable que puede ser optimizado para las tareas de cada operador y ajustarse de acuerdo a las habilidades específicas y niveles de autoridad.

La interfaz le permite adaptar su experiencia de visualización de entornos de trabajo específicos mediante la selección de una luz o un tema oscuro, dependiendo de la iluminación de la habitación o el brillo del vídeo. También cuenta con pestañas optimizado con el trabajo y una línea de tiempo de vídeo integrado para la operación de vigilancia fácil. Con el SDK MIP, los usuarios pueden integrar diversos tipos de sistemas de seguridad y sistemas empresariales y aplicaciones de análisis de video, que gestiona a través de XProtect Smart Client.

XProtect Smart Client debe estar instalado en los ordenadores de los usuarios. Los administradores del sistema de vigilancia administran el acceso de los clientes al sistema de vigilancia a través del Management Client. Grabaciones vistos por los clientes son proporcionados por el servicio Image Server de su sistema XProtect. El servicio se ejecuta en segundo plano en el servidor del sistema de vigilancia. No se requiere hardware separado.

Para descargar XProtect Smart Client, debe conectarse al servidor del sistema de vigilancia que le presenta una página de bienvenida que enumera los clientes disponibles y las versiones de idioma. Los administradores de sistemas pueden utilizar XProtect Download Manager para controlar lo que los clientes y las versiones lingüísticas deberían estar a disposición de los usuarios en la página de bienvenida de la XProtect Download Manager.

Milestone Mobile cliente (explicado)

Milestone Mobile cliente es una solución de vigilancia móvil estrechamente integrado con el resto de su sistema XProtect. Funciona en tu tableta o smartphone Android, tu tablet Apple®, tu smartphone o reproductor de música portátil o tu tablet o teléfono inteligente Windows Phone 8 y te da acceso a cámaras, vistas y otras funciones configuradas en los clientes de administración.

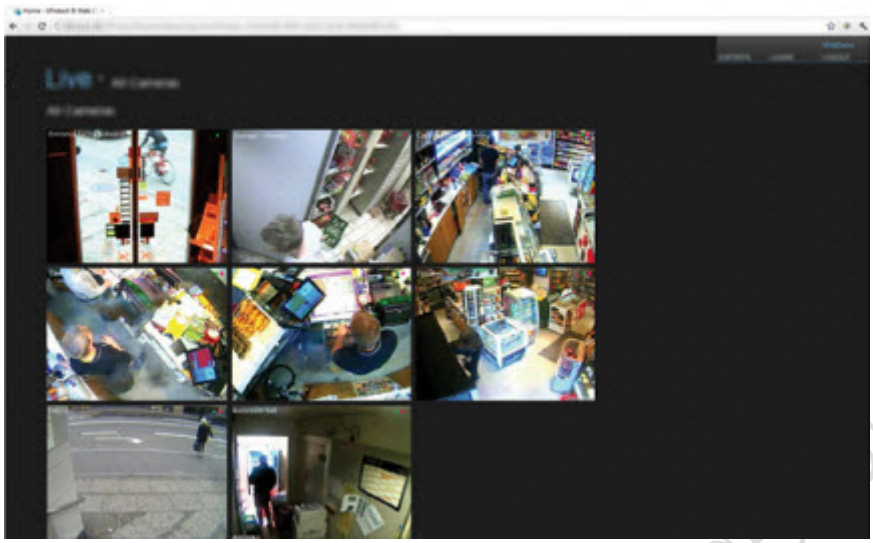
Utilice el cliente de Milestone Mobile para ver y reproducir vídeo en directo y grabado de una o varias cámaras, el control de giro, inclinación y zoom (PTZ), salida de disparo y eventos y utilizar la funcionalidad de vídeo de empuje para enviar vídeo desde el dispositivo a la XProtect sistema.

Si desea utilizar el cliente Milestone Mobile con su sistema, debe tener un servidor Mobile para establecer la conexión entre el cliente Milestone Mobile y su sistema. Una vez que el servidor Mobile está configurado, descargar el cliente de Milestone Mobile de forma gratuita desde Google Play, App Store o la tienda de Windows Phone para empezar a utilizar Milestone Mobile.

Necesitará una licencia de dispositivo de hardware por cada dispositivo que debe ser capaz de empujar a su sistema de vídeo XProtect.

Acerca de XProtect Web Client

XProtect Web Client es una aplicación cliente basada en web para ver, reproducir y compartir vídeos. Proporciona acceso instantáneo a las funciones de vigilancia más comúnmente utilizados, tales como la visualización de vídeo en directo, reproducir el vídeo grabado, impresión y pruebas de exportación. El acceso a las funciones depende de los derechos de los usuarios individuales que se configuran en el cliente de gestión.



Para habilitar el acceso a XProtect Web Client, debe tener un servidor Mobile para establecer la conexión entre XProtect Web Client y su sistema. El XProtect Web Client en sí no requiere ninguna instalación en sí y funciona con la mayoría de los navegadores de Internet. Una vez que haya configurado el servidor de Mobile, puede supervisar el sistema XProtect cualquier lugar desde cualquier ordenador o dispositivo con acceso a Internet (siempre que conozca la dirección de Internet, nombre correcto externa / usuario y contraseña).

Licencias (explicadas)

Si ha instalado su sistema XProtect Essential+, puede ejecutar el sistema y ocho licencias de dispositivo de hardware de forma gratuita. La activación automática de la licencia está activada y el hardware se activará a medida que se añada al sistema.
Solo cuando tu mejorar (ver "Cambiar el código de licencia de software" en la página 51) a un producto XProtect más avanzado, el resto de este tema y los otros temas relacionados con la licencia de esta documentación son relevantes.

Cuando usted compra su software y licencias, usted recibe:

- Una confirmación de pedido.
- Un archivo de licencia de software con el nombre de su SLC (código de licencia de software) y con la extensión .lic.

Su SLC también está impreso en la confirmación de su pedido y consta de varios números y letras agrupadas por guiones como:

- Versión del producto 2014 o anterior: xxx xxxx xxxx
- Versión del producto 2016 o posterior: xxx xxx xxx xxx xxxxxx

El archivo de licencia del software contiene toda la información sobre los productos y licencias VMS adquiridos. Milestone recomienda que almacene la información sobre su SLC y una copia de su archivo de licencia de software en un lugar seguro desde el que pueda volver a encontrarlos. En el árbol de navegación, también se

puede ver su SLC si selecciona **Fundamentos** > **Información de licencia**. Es posible que necesite el archivo de licencia de software o su SLC cuando, por ejemplo, cree una cuenta de usuario My Milestone, póngase en contacto con su distribuidor para obtener asistencia y si necesita realizar cambios en su sistema.

Para empezar, descarga el software desde nuestro sitio web (http://www.milestonesys.com/downloads). Mientras instala (ver "Instalación" en la página 30) el software, se le pide que proporcione el archivo de licencia de software.

Una vez completada la instalación, y tiene activada las licencias, se puede ver un resumen de sus licencias (ver "Información de licencia" en la página 71) para todas las instalaciones en el mismo SLC sobre los **Fundamentos** > página **Información de licencia**.

Ha adquirido como mínimo dos tipos de licencias:

Licencias base: Como mínimo, tiene una licencia de base para uno de los productos XProtect. Usted también puede tener una o más bases licencias para XProtect productos adicionales.

Licencias de dispositivo de hardware: Cada dispositivo de hardware que se agrega a su sistema XProtect requiere una licencia de dispositivo de hardware. No necesita licencias de dispositivos de hardware para altavoces, micrófonos o dispositivos de entrada y salida conectados a sus cámaras. Sólo necesita licencia de dispositivo de hardware uno por cada dirección IP codificador de vídeo, incluso si conecta varias cámaras para el codificador de vídeo. Un codificador de vídeo puede tener una o más direcciones IP.

Para obtener más información, consulte la lista de hardware compatible en el sitio web Milestone (https://www.milestonesys.com/supported-devices). Si desea utilizar la función de inserción de vídeo en Milestone Mobile, también necesitará una licencia de dispositivo de hardware por dispositivo móvil o tableta que debería poder empujar video a su sistema. Si se queda sin licencias de dispositivo de hardware, puede desactivar (ver "Desactivar / activar el hardware" en la página 110) los dispositivos de hardware menos importantes para permitir que se ejecuten nuevos dispositivos de hardware.

Si su sistema de vigilancia es el sitio central de una jerarquía del sistema de mayor tamaño usando Milestone Interconnect, necesita licencias de cámara de Milestone Interconnect para poder ver el vídeo de los dispositivos de hardware en sitios remotos. Tenga en cuenta que XProtect Corporate como instalación central.

La mayoría de los productos add-on XProtect requieren tipos de licencia adicionales. El archivo de licencia de software también incluye información sobre las licencias para productos add-on. Algunos productos add-on tienen sus propios archivos de licencia de software independientes. Puede encontrar más información acerca de Licencias de producto aquí:

- XProtect Access (ver "Licencias XProtect Access" en la página 329)
- XProtect LPR (ver "Licencias XProtect LPR" en la página 339)
- XProtect Transact (ver "Primeros pasos" en la página 376)
- XProtect Smart Wall (ver "Licencias XProtect Smart Wall" en la página 322) (incluido en XProtect Corporate)
- Para las licencias de producto complementario para XProtect Retail y XProtect Screen Recorder, consulte la documentación de estos productos.

Tabla de comparación de productos

XProtect VMS incluye los siguientes productos:

- XProtect Corporate

- XProtect Expert
- XProtect Professional+
- XProtect Express+
- XProtect Essential+

La lista completa de funciones está disponible en la página descripción del producto en la página web de Milestone (https://www.milestonesys.com/solutions/platform/product-index/).

A continuación se muestra una lista de las principales diferencias entre los productos:

Nombre	XProtect Essential+	XProtect Express+	XProtect Professional+	XProtect Expert	XProtect Corporate
Sitios por SLC	1	1	Multi-sitio	Multi-sitio	Multi-sitio
Grabación de servidores por SLC	1	1	Irrestricto	Irrestricto	Irrestricto
Dispositivos de hardware por servidor de grabación	8	48	Irrestricto	Irrestricto	Irrestricto
Milestone Interconnect™	-	Ubicación remota	Ubicación remota	Ubicación remota	Ubicación central/remota
Milestone Federated Architecture™	-	-	-	Ubicación remota	Ubicación central/remota
Grabación de la conmutación por error del servidor	-	-	-	Tiempo de espera frío y caliente	Tiempo de espera frío y caliente
Servicios de conexión remota	-	-	-	-	✓
Soporte de almacenamiento de bordes	-	-	✓	✓	✓
Migración de servidores de códigos electrónicos	✓	✓	✓	✓	✓
Almacenamiento de vídeo multietapa	Bases de datos en vivo + 1 archivo	Bases de datos en vivo + 1 archivo	Bases de datos en vivo + 1 archivo	Archivos sin restricciones de bases de datos en vivo	Archivos sin restricciones de bases de datos en vivo
Notificación SNMP	-	-	-	✓	✓
Derechos de acceso de usuario con tiempo controlado	-	-	-	-	✓
Reducir velocidad de fotogramas (limpieza)	-	-	-	✓	✓

Nombre	XProtect Essential+	XProtect Express+	XProtect Professional+	XProtect Expert	XProtect Corporate
Cifrado de datos de vídeo (servidor de grabación)	-	-	-	✓	✓
Acceso a la base de datos (servidor de grabación)	-	-	-	✓	✓
Niveles de prioridad PTZ	1	1	3	32000	32000
PTZ extendida (reserva de la sesión PTZ y patrullaje desde XProtect Smart Client)	-	-	-	✓	✓
Bloqueo de evidencias	-	-	-	-	✓
Función de marcador	-	-	Solo manual	Manual y basada en reglas	Manual y basada en reglas
Multi-streaming en vivo / multidifusión	-	-	-	✓	✓
Seguridad general	Derechos de usuario del cliente	Derechos de usuario del cliente	Derechos de usuario del cliente	Derechos de usuario del cliente	Derechos de usuario del cliente/ derechos de usuario del administrador
Los perfiles XProtect Management Client	-	-	-	-	✓
Perfiles de XProtect Smart Client	-	-	3	3	Irrestricto
XProtect Smart Wall	-	-	-	opcional	✓
Monitor de sistema	-	-	-	✓	✓
Plano inteligente	-	-	-	✓	✓
Doble verificación de acceso	-	-	-	-	✓
Soporte DLNA	-	✓	✓	✓	✓
Máscara de privacidad	-	✓	✓	✓	✓

IPv6 e IPv4 (explicado)

El sistema admite IPv6, así como IPv4. Lo mismo ocurre con XProtect Smart Client.

IPv6 es la última versión del Protocolo de Internet (IP). El protocolo de Internet determina el formato y el uso de direcciones IP. IPv6 coexiste con la versión de IP sigue siendo mucho más ampliamente utilizado IPv4. IPv6 se desarrolló con el fin de resolver el agotamiento de las direcciones de IPv4. Las direcciones IPv6 son 128 bits de largo, mientras que las direcciones IPv4 son solamente 32 bits de longitud.

Significaba que la libreta de direcciones de Internet creció de 4.300 millones de direcciones únicas a 340 direcciones de undecilion (340 billones de billones de trillones). Un factor de crecimiento del 79 octillion (billones de billones de billones).

Cada vez más organizaciones están implementando IPv6 en sus redes. Por ejemplo, se requiere que todas las infraestructuras de las agencias federales de Estados Unidos para ser compatible con IPv6. Ejemplos e ilustraciones de este manual reflejan el uso de IPv4, porque esto sigue siendo la versión de IP más utilizado. IPv6 funciona igual de bien con el sistema.

Uso del sistema con IPv6 (explicado)

Las siguientes condiciones se aplican al utilizar el sistema con IPv6:

Servidores

Menudo, los servidores pueden utilizar IPv4 como IPv6. Sin embargo, si sólo un servidor en el sistema (por ejemplo, un servidor de gestión o servidor de grabación) requiere una versión IP en particular, todos los demás servidores de su sistema deben comunicarse usando la misma versión de IP.

> **Ejemplo**: Todos los servidores de su sistema, salvo que uno puede utilizar IPv4 como IPv6. La excepción es un servidor que sólo es capaz de utilizar IPv6. Esto significa que todos los servidores deben comunicarse entre sí utilizando IPv6.

Dispositivos

Es posible utilizar dispositivos (cámaras, entradas, salidas, micrófonos, altavoces) con una versión de IP diferente al que está siendo utilizado para la comunicación servidor proporcionado el equipo de red y los servidores de grabación también apoyar IP versión de los dispositivos. Ver también la siguiente ilustración.

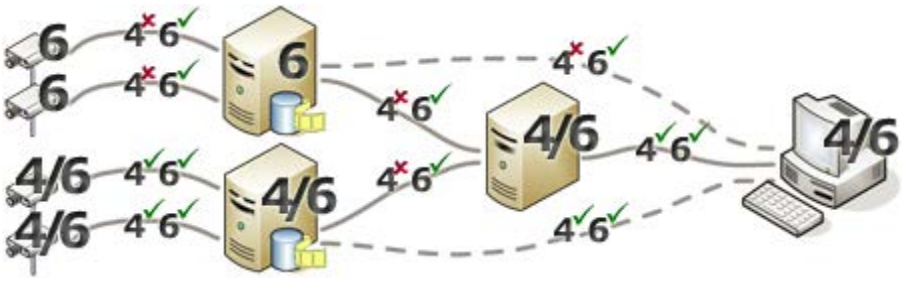
Clientes

Si el sistema utiliza IPv6, los usuarios deben conectar con el XProtect Smart Client. El XProtect Smart Client es compatible con IPv6, así como IPv4.

Si uno o más servidores en su sistema pueden **sólo** utilizar IPv6, XProtect Smart Client usuarios **deben** utilizar IPv6 para su comunicación con esos servidores. En este contexto, es importante recordar que los XProtect Smart Clients técnicamente se conectan a un servidor de gestión para la autenticación inicial, y luego a los servidores de grabación requeridas para el acceso a las grabaciones.

Sin embargo, los usuarios de XProtect Smart Client no tienen que estar en una red IPv6 a sí mismos, siempre y cuando su equipo de red soporta la comunicación entre las diferentes versiones de IP, y han instalado el protocolo IPv6 en sus equipos. Ver también la ilustración. Para instalar IPv6 en un equipo cliente, abra un símbolo del sistema, escriba Ipv6 instalar, y pulse **ENTER**.

Ilustración a modo de ejemplo



Ejemplo: Desde un servidor en el sistema sólo puede utilizar IPv6, todas las comunicaciones con dicho servidor debe utilizar IPv6. Sin embargo, ese servidor también determina la versión de IP para. La comunicación entre todos los demás servidores del sistema.

Sin compatibilidad de Matrix Monitor

Si se utiliza IPv6, no se puede utilizar la aplicación Matrix Monitor con su sistema. Funcionalidad de Matrix en XProtect Smart Client no se ve afectada.

Escribir direcciones IPv6 (explicadas)

Una dirección IPv6 se escribe generalmente como ocho bloques de cuatro dígitos hexadecimales, con cada bloque separado por dos puntos.

Ejemplo: 2001:0B80:0000:0000:0000:0F80:3FA8:18AB

Es posible acortar direcciones mediante la eliminación de ceros a la izquierda en un bloque. Además, tenga en cuenta que algunos de los bloques de cuatro dígitos pueden consistir únicamente en ceros. Si cualquier número de tales bloques 0000 son consecutivas, es posible acortar direcciones mediante la sustitución de los bloques 0000 con dos signos de dos puntos, siempre y cuando no hay más que uno de esos dos puntos dobles en la dirección.

Ejemplo:
2001:0B80:0000:0000:0000:0F80:3FA8:18AB puede acortarse a

2001:B80:0000:0000:0000:F80:3FA8:18ABsi quita los ceros a la izquierda o

2001:0B80::0F80:3FA8:18AB si la eliminación de los bloques 0000, o incluso a

2001:B80::F80:3FA8:18AB si la eliminación de los ceros a la izquierda, así como los bloques 0000.

El uso de direcciones IPv6 en las direcciones URL

Las direcciones IPv6 contienen dos puntos. Los dos puntos, sin embargo, también se utilizan en otros tipos de red sintaxis de direccionamiento. Por ejemplo, IPv4 utiliza dos puntos para separar la dirección IP y número de puerto cuando ambos se utilizan en una dirección URL. IPv6 ha heredado este principio. Por lo tanto, para evitar la confusión, los corchetes se ponen alrededor de las direcciones IPv6 cuando se utilizan en las URL.

Ejemplo de una URL con una dirección IPv6:
http://[2001:0B80:0000:0000:0000:0F80:3FA8:18AB], Que se puede acortar, por supuesto, a, por ejemplo, http://[2001:B80::F80:3FA8:18AB]

Ejemplo de una URL con una dirección IPv6 y un número de puerto:
http://[2001:0B80:0000:0000:0000:0F80:3FA8:18AB]:1234, Que se puede acortar, por supuesto, a, por ejemplo, http://[2001:B80::F80:3FA8:18AB]:1234

Para obtener más información acerca de IPv6, consulte, por ejemplo, el sitio web IANA (http://www.iana.org/numbers/). IANA, la Autoridad de Números Asignados de Internet (Internet Assigned Numbers Authority) , es la organización responsable de la coordinación global de direccionamiento IP.

Requisitos del sistema

Importante: El sistema ya no admite Microsoft® Windows® 2008 pero pueden seguir ejecutándose los clientes o se puede seguir accediendo a ellos desde ordenadores con Windows 2008.

Importante: El sistema ya no admite Microsoft® Windows® de 32 bits pero pueden seguir ejecutándose o acceder a XProtect Web Client y XProtect Smart Client desde ordenadores con Windows de 32 bits.

Para obtener información acerca de los requisitos **mínimos** del sistema para los diversos componentes de su sistema, consulte la Milestone página web (https://www.milestonesys.com/support/resources/system-requirements).

Instalación

Si actualiza desde una versión anterior XProtect, consulte Actualización (explicada) (ver "Actualización (explicado)" en la página 59).

Antes de comenzar la instalación

Milestone recomienda que consulte los requisitos descritos en las siguientes secciones antes de comenzar la propia instalación.

Preparar sus servidores y red

Sistema operativo

Asegúrese de que todos los servidores tienen una instalación limpia de un operativo Microsoft Windows, y que está actualizada con todas las actualizaciones de Windows.

Para obtener información acerca de los requisitos **mínimos** del sistema para los diversos componentes de su sistema, consulte el sitio web (https://www.milestonesys.com/support/resources/system-requirements) de Milestone.

Microsoft® .NET framework

Compruebe que todos los servidores poseen Microsoft .NET 4.7 framework o superior instalado.
Compruebe que el servidor objetivo de la instalación del servidor de gestión tiene instalado Microsoft .NET 3.5 SP1 framework. Esto es un requisito del servidor SQL.

Red

Asignar direcciones IP estáticas o hacer reservas DHCP en todos los componentes del sistema y cámaras. Para asegurarse de que hay suficiente ancho de banda disponible en la red, debe saber cuándo y cómo el uso del sistema consume ancho de banda. La cara principal de la red consiste en tres elementos:

- Flujos de vídeo de cámara
- Clientes proyectando vídeo
- Archivado de vídeo grabado

El servidor de grabación recupera flujos de vídeo desde las cámaras que resulta en una carga constante en la red. Los clientes que proyectan vídeo consumen ancho de banda de la red. Si no hay cambios en el contenido de las vistas del cliente, la carga es constante. Los cambios en el contenido de las vistas, búsquedas de vídeo o reproducciones, hace que la carga sea dinámica.

El archivado de grabaciones de vídeo es una función opcional que permite al sistema trasladar grabaciones a unidades de almacenamiento de red si no hay suficiente espacio en el almacenamiento interno del ordenador. Esto es una tarea programada que tiene que definir. Normalmente, se archiva en una unidad de red que la convierte en una carga dinámica en la red.

La red debe poseer espacio en el ancho de banda para gestionar estas subidas en el tráfico. De este modo se intensifica el rendimiento del sistema y la experiencia de usuario en general.

Prepare Active Directory

Si desea agregar usuarios a su sistema a través del servicio Active Directory, debe tener un servidor con Active Directory instalado que actúe como controlador de dominio disponible en su red.

Para una gestión fácil de grupos y usuarios, Milestone recomienda que tenga instalado y configurado Microsoft Active Directory® antes de instalar el sistema XProtect. Si añade el servidor de gestión a Active Directory después de reinstalar su sistema, deberá reinstalar el servidor de gestión y remplazar los usuarios con los nuevos usuarios de Windows definidos en Active Directory.

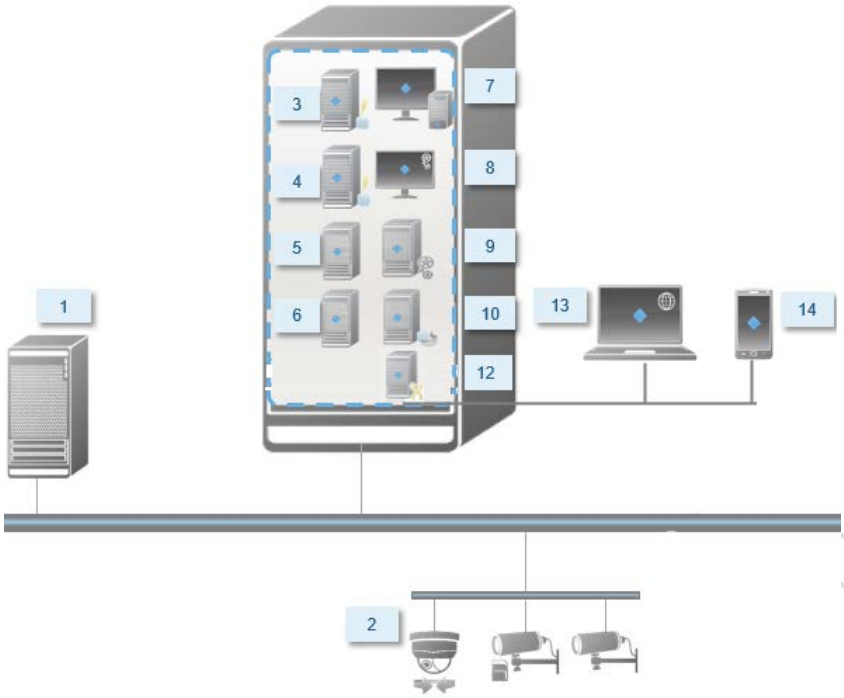
Los usuarios básicos no se admiten en sistemas Milestone Federated Architecture, así que si tiene intención de incluir usuarios básicos en su sistema, debe añadirlos a través del servicio Active Directory. Si no instala Active Directory, siga estos pasos en Instalación para grupos de trabajo (ver "Instalación de grupos de trabajo" en la página 48) cuando los instale.

Método de instalación

Como parte del asistente de instalación, debe decidir qué método quiere usar. Debe basar su selección en las necesidades de su organización, pero es probable que ya lo haya hecho al adquirir el sistema.

Opciones	Descripción
Ordenador único	Instala todos los componentes del servidor de gestión, servidor de grabación, servidor Milestone Mobile, y XProtect Smart Client, así como el servidor SQL en el equipo actual. La instalación de ordenador único instala y configura el sistema. Se autoriza el servidor de grabación, y ya está listo para usar el sistema inmediatamente después de la instalación. Según el hardware y la configuración, el servidor de grabación escanea la red en busca del hardware, añade 64 piezas de hardware automáticamente, que después se añaden a su sistema. Las cámaras tienen vistas preconfiguradas y se crea un rol de Operador predeterminado. Después de la instalación, abra XProtect Smart Clienty ya está listo para utilizar el sistema.
Distribuido	Instala solo los componentes del servidor de gestión en el equipo actual. Esto significa que el servidor de grabación XProtect Smart Client no está visible en la lista de componentes. No puede editar nada en la lista de componentes. Debe instalar el servidor de grabación, servidor Milestone Mobile y XProtect Smart Client en otros equipos.
Custom (personalizada)	El servidor de gestión siempre está seleccionado en la lista de componentes del sistema, y siempre se instala, pero puede seleccionar libremente qué quiere instalar en el equipo actual, como los otros componentes del servidor de gestión, el servidor de grabación y XProtect Smart Client. De manera predeterminada, el servidor de grabación se elimina de la lista de componentes, pero esto se puede modificar. Según las elecciones que haya tomado, después debe instalar los componentes seleccionados en otros equipos.

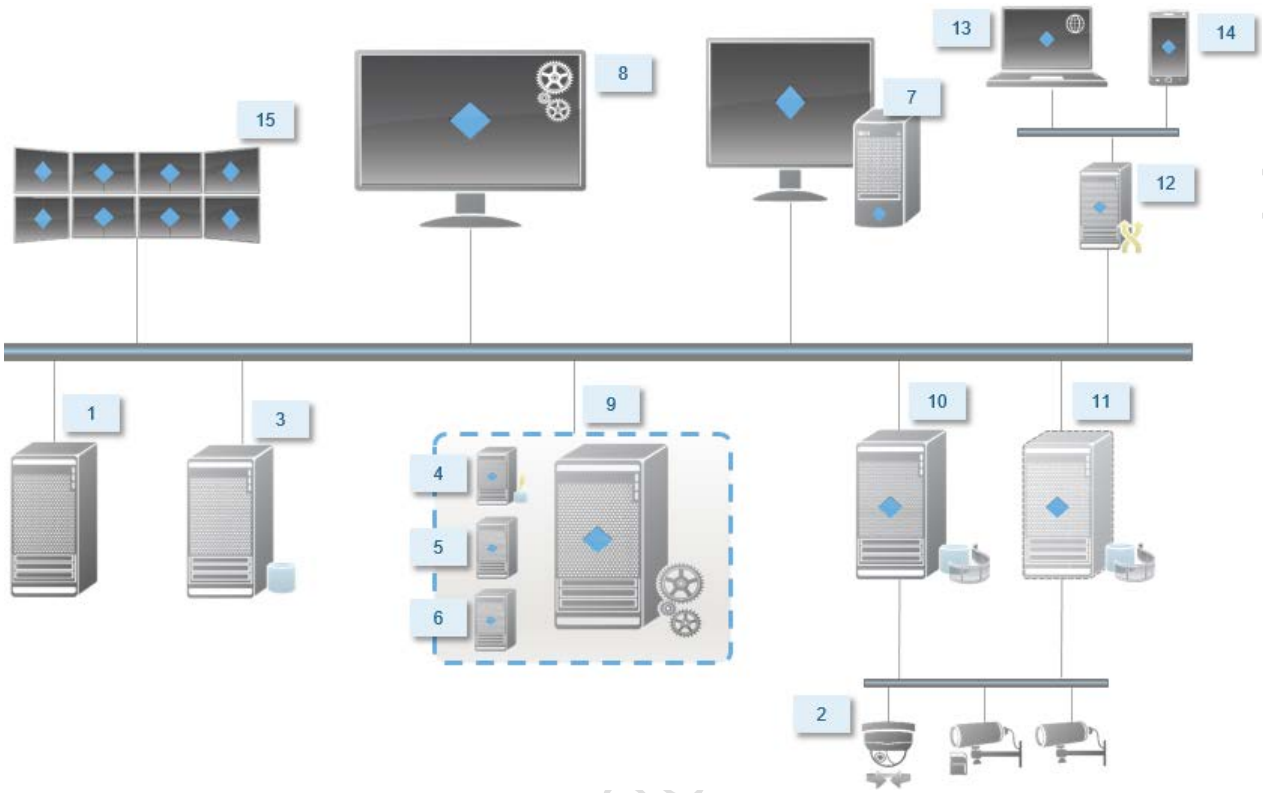
Instalación de ordenador único



Componentes de sistema en un sistema habitual:

1. **Active Directory**
2. **Dispositivos**
3. **Servidor SQL**
4. **Servidor de eventos**
5. **Servidor de registro**
6. **Canal de servicio**
7. **XProtect Smart Client**
8. **Management Client**
9. **Servidor de gestión**
10. **Servidor de grabación**
11. **Servidor de grabación failover**
12. **Servidor Milestone Mobile**
13. **XProtect Web Client**
14. **Cliente Milestone Mobile**
15. **XProtect Smart Client con XProtect Smart Wall**

Instalación distribuida



Determinar el tipo de servidor SQL.

Microsoft SQL Server Express Edition es una versión «light» de un servidor SQL completo. Es fácil de instalar y preparar para su uso y a menudo es una buena opción para sistemas con menos de 300 cámaras. Esta versión del servidor SQL se incluye en la instalación de un **ordenador único**.

Para instalaciones con más de 300 cámaras, Milestone recomienda usar un servidor SQL dedicado en un equipo dedicado en red. Debe tener derechos de administrador en el servidor SQL.

Milestone recomienda instalar la base de datos en una unidad de disco duro específica que no se utilice para nada más. La instalación de la base de datos en su propia unidad mejora el rendimiento general del sistema.

Cuando seleccione **Distribuida** o **Personalizada** como parte del asistente de instalación, debe decidir qué hacer con respecto al servidor SQL.

Si no tiene el servidor SQL instalado, las opciones son:

- **Instalar SQL Server Express en este equipo**.
- **Usar un servidor SQL Server existente en red:** Si su sistema usa un equipo dedicado para la base de datos SQL, aparece la lista de servidores SQL a la que puede acceder.

Si tiene el servidor SQL instalado, las opciones son:

- **Usar la base de datos Microsoft SQL Server Express instalada en este equipo.**
- **Usar un servidor SQL Server existente en red:** Cuando usa un equipo dedicado para la base de datos SQL en la red, aparece la lista de servidores SQL a la que puede acceder.

  También se le preguntará si quiere crear una nueva base de datos, utilizar una base de datos existente o sobrescribir una base de datos existente.

- **Crear una nueva base de datos:** Para una instalación nueva.
- **Usar base de datos existente:** Si está instalando la base de datos como parte de la actualización del sistema y quiere utilizar su base de datos existente.

Seleccionar la cuenta de servicio

Como parte de la instalación, se le pide que especifique una cuenta para ejecutar los servicios de Milestone en este equipo. Los servicios siempre se ejecutan en esta cuenta sin tener en cuenta qué usuario ha iniciado sesión. Asegúrese de que la cuenta posee todos los derechos de usuario necesario, por ejemplo, la red y el acceso de archivos adecuado, y acceso a las carpetas de red compartidas.

Puede seleccionar una cuenta predefinida, o una cuenta de usuario. Su decisión se debe basar en el entorno en que quiere instalar su sistema:

Entorno de dominio

En un entorno de dominio:

- Milestone recomienda que use la cuenta de Servicio de Red integrada. Es más fácil de usar incluso si tiene que ampliar el sistema a varios equipos.
- También puede usar las cuentas de usuario de dominio, pero son potencialmente más difíciles de configurar.

Entorno de grupo de trabajo

En un entorno de grupo de trabajo, Milestone recomienda que use una cuenta de usuario local que pose todos los derechos. Esta a veces es la cuenta de administrador.

Importante: Si sus instalaciones cubren varios equipos, la cuenta de usuario seleccionada debe existir en todos los equipos de la instalación con los mismos nombres de usuario, contraseña y derechos de acceso.

Autenticación Kerberos (explicada)

Kerberos es un protocolo de autenticación de red basada en la compra de entradas. Está diseñado para proporcionar una autenticación fuerte para el cliente / servidor o aplicaciones de servidor / servidor.

Utilizar la autenticación Kerberos como una alternativa al protocolo de autenticación anteriores Microsoft NT LAN (NTLM).

La autenticación Kerberos requiere autenticación mutua, donde el cliente se autentica en el servicio y el servicio autentica al cliente. De esta manera se puede autenticar de forma más segura desde XProtect clientes a servidores XProtect sin exponer su contraseña.

Para que la autenticación mutua sea posible en su VMS XProtect, debe registrar los nombres principales de servicio (SPN) en el directorio activo. Un SPN es un alias que identifica de forma única una entidad como un servicio XProtect servidor. Cada servicio que utiliza la autenticación mutua debe tener un SPN registrado para que los clientes puedan identificar el servicio en la red. Sin SPN correctamente registrados, autenticación mutua no es posible.

La siguiente tabla muestra los diferentes Milestone servicios con números de puerto correspondientes que necesita para registrarse:

Servicio	Número de puerto
Servidor de administración - IIS	80 - Configurable
Servidor de administración - Interno	8080
Grabación de servidor - Data Collector	7609
Serveur de redondance	8990
Servidor de eventos	22331
Servidor LPR	22334

El número de servicios que usted necesita colocarse en el directorio activo depende de la instalación actual. Data Collector se instala automáticamente al instalar Servidor de administración, Servidor de grabación, Servidor de eventos, Servidor LPR o Servidor de conmutación por error.

Debe registrar dos SPN para el usuario que ejecuta el servicio: una con el nombre de host y una con el nombre de dominio completo.

Si está ejecutando este servicio con una cuenta de servicio de usuario de la red, debe registrar los dos SPN para cada equipo que ejecuta este servicio.

Este es el esquema de nombres Milestone SPN:
VideoOS / [nombre de host DNS]: [puerto]
VideoOS / [nombre completo de dominio]: [puerto]

El siguiente es un ejemplo de SPN para el servicio de servidor de grabación que se ejecuta en un ordenador con los siguientes detalles:
Nombre de host: Registros del servidor 1
Dominio: Surveillance. com

SPN para registrar:
VideoOS / Record-Server1: 7609
VideoOS / Record-Server1.Surveillance.com: 7609

Exploración de virus (explicada)

Como ocurre con cualquier otro software de base de datos, si un programa antivirus está instalado en un equipo que ejecuta el software XProtect, es importante que excluya tipos y carpetas de archivos específicos, así como cierto tráfico de red. Sin implementar estas excepciones, el análisis de virus utiliza una cantidad considerable de recursos del sistema. Además, el proceso de análisis puede bloquear temporalmente los archivos, lo que podría provocar una interrupción en el proceso de grabación o incluso la corrupción de las bases de datos.

Cuando necesite realizar análisis de virus, no explore las carpetas del servidor de grabación que contengan bases de datos de grabación (por defecto C:\mediadatabase\, así como todas las subcarpetas). Además, evite realizar análisis de virus en los directorios de almacenamiento de archivos.

Cree las siguientes exclusiones adicionales:

- Tipos de archivo: .blk, .idx, .pic

- Carpetas y subcarpetas:
  - C:\Program Files\Milestone or C:\Program Files (x86)\Milestone
  - C:\ProgramData\Milestone\MIPSDK
  - C:\ProgramData\Milestone\Milestone Mobile Server\Logs
  - C:\ProgramData\Milestone\XProtect Data Collector Server\Logs
  - C:\ProgramData\Milestone\XProtect Event Server\logs
  - C:\ProgramData\Milestone\XProtect Log Server
  - C:\ProgramData\Milestone\XProtect Management Server\Logs
  - C:\ProgramData\Milestone\XProtect Recording Server\Logs
  - C:\ProgramData\Milestone\XProtect Report Web Server\Logs
  - C:\ProgramData\Milestone\XProtect Service Channel\Logs
- Excluya la exploración de red en los siguientes puertos TCP:

Producto	Puertos TCP
XProtect VMS	80, 8080, 7563, 25, 21, 9993
Milestone Mobile	8081

o

- Excluya el escaneado en red de los siguientes procesos:

Producto	Procesos
XProtect VMS	VideoOS.Recording.Service.exe, VideoOS.Server.Service.exe, VideoOS.Administration.exe
Milestone Mobile	VideoOS.MobileServer.Service.exe

Es posible que su organización tenga directrices estrictas con respecto a la detección de virus, pero es importante que excluya las carpetas y archivos anteriores de la detección de virus.

Registrar el código de licencia de software

Antes de la instalación, debe tener el nombre y la ubicación del archivo de licencia de software que ha recibido de Milestone.

Puede instalar la versión gratuita de XProtect Essential+. Esta versión le proporciona funcionalidad restringida y un número limitado de cámaras, en comparación con el sistema XProtect VMS de pago. En este caso, la licencia se proporciona con el instalador.

El código de licencia de software (SLC) está impreso en la confirmación del pedido y el archivo de licencia de software lleva el nombre de su SLC. Milestone recomienda que registre su SLC en su página web (http://online.milestonesys.com) antes de instalarlo. Es posible que el distribuidor ya lo haya hecho.

Requisitos para la instalación sin conexión

Si instala el sistema en un servidor que está fuera de línea, es necesario lo siguiente:

- El archivo `Milestone XProtect VMS Products 2018 R2 System Installer.exe`.
- El archivo de licencia de software (SLC) para su sistema XProtect.
- Medio de instalación del sistema operativo que incluye la versión .NET requerido (https://www.milestonesys.com/support/resources/system-requirements).

Instale el sistema

Seleccione una de las opciones de instalación:

- Instalar su sistema - XProtect Essential+ (en la página 37)
- Instalar su sistema - Opción de Equipo único (ver "Instale su sistema - Opción Único equipo" en la página 39)
- Instalar su sistema - Opción distribuida (ver "Instalar el sistema - Opción de distribución" en la página 41)
- Instalar el sistema - Opción personalizada (ver "Instalar el sistema - Opción de personalización" en la página 42)

Instalar su sistema - XProtect Essential+

Puede instalar una versión gratuita de XProtect Essential+. Esta versión le proporciona capacidades limitadas de XProtect VMS para un número limitado de cámaras. Debe tener conexión a Internet para instalar XProtect Essential+.

Esta versión se instala en una sola computadora, utilizando la opción de instalación **Único equipo** . La opción **Único equipo** instala todos los componentes de servidor y cliente en la computadora actual. El servidor de grabación está autorizado, por lo que está listo para utilizar el sistema directamente después de la instalación.

Después de la instalación inicial, puede continuar con el asistente de configuración. Dependiendo de su hardware y configuración, el servidor de grabación escanea su red en busca de hardware. A continuación, puede seleccionar qué piezas de hardware agregar a su sistema. Las cámaras están preconfiguradas en vistas, y tiene la opción de habilitar otros dispositivos como micrófonos y parlantes. También tiene la opción de agregar usuarios al rol de Operadores o Administradores. Después de la instalación, se abre XProtect Smart Client y ya está listo para utilizar el sistema.

De lo contrario, si cierra el asistente de instalación, se abre XProtect Management Client, donde puede realizar configuraciones manuales, como agregar hardware y usuarios al sistema.

Microsoft® IIS se instala automáticamente durante el proceso.Posteriormente, se le pedirá que reinicie el equipo.Haga esto y después de reiniciar, dependiendo de su configuración de seguridad, una o más advertencias de seguridad de Windows pueden aparecer.Acepte estos y la instalación completa.

Nota: Si actualiza desde una versión anterior del producto, el sistema no busca hardware o crea nuevas vistas y perfiles de usuario.

1. Descargue el software desde Internet (http://www.milestonesys.com/downloads) y ejecute el archivo `Milestone XProtect VMS Products 2018 R2 System Installer.exe` desde la ubicación donde lo guardó.
2. Los archivos de instalación se desempaquetan.En función de la configuración de seguridad, aparecerán una o varias advertencias de seguridad de Windows ®.Acepte estos y el desembalaje continúa.
3. Cuando haya terminado, el cuadro de diálogo **Milestone XProtect VMS** aparece,
    1. Seleccione **Idioma** para usar durante la instalación (esto es **no** el idioma que su sistema utiliza una vez instalado, esto se selecciona más adelante).Haga clic en **Continuar**.
    2. Lea el Milestone Contrato de licencia de usuario final.Seleccione la casilla de verificación **Acepto los términos del contrato de licencia** y haga clic en **Continuar**.
    3. Haga clic en **Descarga gratuita XProtect Essential+ licencia**.

        La licencia gratuita se descarga y aparece en el campo del archivo de licencia.Haga clic en **Continuar**.
4. Seleccione **Ordenador único**.

    Aparece una lista de todos los componentes a instalar (esta lista no se puede modificar). Haga clic en **Continuar**.
5. En la ventana de **Especificar la configuración del servidor de grabación**, haga lo siguiente:
    1. En el campo de **Nombre del servidor de grabación**, introduzca el nombre del servidor de grabación. El valor predeterminado es el nombre del equipo.
    2. El campo de **Dirección del servidor de gestión** muestra la dirección y número de puerto del servidor de gestión: localhost:80.
    3. En el campo de **Seleccionar la ubicación de su base de datos multimedia**, seleccione la ubicación donde desee guardar la grabación de vídeo. Le recomendamos que guarde las grabaciones de vídeo en una ubicación distinta de donde haya instalado el programa. La ubicación predeterminada es la unidad con más espacio disponible.
    4. En **Período de retención para las grabaciones de vídeo**, defina durante cuánto tiempo desea guardar las grabaciones de vídeo. Puede introducir entre 1 y 999 días, donde 7 días es el periodo de retención predeterminado.
    5. Haga clic en **Continuar**.
6. En la ventana **Seleccionar la ubicación de los archivos y el idioma del producto**, haga lo siguiente:
    1. En el campo **Ubicación del archivo**, seleccione la ubicación donde desee instalar el programa.
    2. En **Idioma del producto**, seleccione el idioma en que quiere instalar su producto XProtect.
    3. Haga clic en **Install** (instalar).

        El software se instala.
7. Cuando se haya completado la instalación, aparece una lista de los componentes instalados en el ordenador.

Haga clic en **Continuar** para añadir hardware y usuarios al sistema.

Nota: Si hace clic en **Cerrar en este momento**, omitirá el asistente de configuración y se abrirá el XP MC. Puede configurar opciones como, por ejemplo, añadir hardware y usuarios al sistema en el MC.

8. En la ventana **Introducir contraseñas y nombres de usuario para el hardware**, introduzca los nombres de usuario y contraseñas para el hardware que haya modificado de los predeterminados de fábrica.

   El programa de instalación escaneará la red en busca de este hardware, así como para el hardware con credenciales predeterminados de fábrica.

   Haga clic en **Continuar**.

9. En la ventana **Seleccione el hardware que quiere agregar al sistema**, selecciona el hardware que desee añadir al sistema. Haga clic en **Continuar**.

10. En la ventana **Configurar los dispositivos**, puede cambiar el nombre del hardware por uno más útil haciendo clic en el icono de edición junto al nombre del hardware. Este nombre precederá a los dispositivos de hardware.

    Expanda el nodo de hardware para habilitar o deshabilitar dispositivos de hardware como cámaras, altavoces y micrófonos.

    Nota: Las cámaras están habilitadas por defecto, y los altavoces y micrófonos están deshabilitados.

    Haga clic en **Continuar**.

11. En la ventana **Añadir usuarios**, puede añadir usuarios de Windows o usuarios básicos. Estos usuarios pueden cumplir el cometido de Administradores o de Operadores.

    Defina el usuario y haga clic en **Añadir**.

    Cuando haya terminado de añadir usuarios, haga clic en **Continuar**.

Cuando haya completado la instalación y la configuración inicial, aparecerá la ventana **Configuración completada**, donde verá:

- Una lista de las cámaras y dispositivos añadidos a su sistema
- Una lista de los usuarios añadidos a su sistema
- Direcciones al servidor WebCName_XP y Mob_comORbrand, que puede copiar y compartir con sus usuarios

Cuando haga clic en **Cerrar**, el SC_XP se abre y está listo para usar.

Instale su sistema - Opción Único equipo

La opción **Único equipo** instala todos los componentes de servidor y cliente en la computadora actual. El servidor de grabación está autorizado, por lo que está listo para utilizar el sistema directamente después de la instalación.

Después de la instalación inicial, puede continuar con el asistente de configuración. Dependiendo de su hardware y configuración, el servidor de grabación escanea su red en busca de hardware. A continuación, puede seleccionar qué piezas de hardware agregar a su sistema. Las cámaras están preconfiguradas en vistas, y tiene la opción de habilitar otros dispositivos como micrófonos y parlantes. También tiene la opción de agregar usuarios al rol de Operadores o Administradores. Después de la instalación, se abre XProtect Smart Client y ya está listo para utilizar el sistema.

De lo contrario, si cierra el asistente de instalación, se abre XProtect Management Client, donde puede realizar configuraciones manuales, como agregar hardware y usuarios al sistema.

Microsoft® IIS se instala automáticamente durante el proceso.Posteriormente, se le pedirá que reinicie el equipo.Haga esto y después de reiniciar, dependiendo de su configuración de seguridad, una o más advertencias de seguridad de Windows pueden aparecer.Acepte estos y la instalación completa.

Nota: Si actualiza desde una versión anterior del producto, el sistema no busca hardware o crea nuevas vistas y perfiles de usuario.

1. Descargue el software desde Internet (http://www.milestonesys.com/downloads) y ejecute el archivo `Milestone XProtect VMS Products 2018 R2 System Installer.exe` desde la ubicación donde lo guardó.
2. Los archivos de instalación se desempaquetan.En función de la configuración de seguridad, aparecerán una o varias advertencias de seguridad de Windows ®.Acepte estos y el desembalaje continúa.
3. Cuando haya terminado, el cuadro de diálogo **Milestone XProtect VMS** aparece,
    1. Seleccione **Idioma** para usar durante la instalación (esto es **no** el idioma que su sistema utiliza una vez instalado, esto se selecciona más adelante).Haga clic en **Continuar**.
    2. Lea el Milestone Contrato de licencia de usuario final.Seleccione la casilla de verificación **Acepto los términos del contrato de licencia** y haga clic en **Continuar**.
4. En **Escriba o busque la ubicación del archivo de licencia**, ingrese su archivo de licencia de su proveedor de XProtect. Como alternativa, utilice la función de exploración para localizarlo. El sistema verifica el archivo de licencia antes de poder continuar. Haga clic en **Continuar**.
5. Seleccione **Ordenador único**.

    Aparece una lista de todos los componentes a instalar (esta lista no se puede modificar). Haga clic en **Continuar**.
6. En la ventana de **Especificar la configuración del servidor de grabación**, haga lo siguiente:
    1. En el campo de **Nombre del servidor de grabación**, introduzca el nombre del servidor de grabación. El valor predeterminado es el nombre del equipo.
    2. El campo de **Dirección del servidor de gestión** muestra la dirección y número de puerto del servidor de gestión: localhost:80.
    3. En el campo de **Seleccionar la ubicación de su base de datos multimedia**, seleccione la ubicación donde desee guardar la grabación de vídeo. Le recomendamos que guarde las grabaciones de vídeo en una ubicación distinta de donde haya instalado el programa. La ubicación predeterminada es la unidad con más espacio disponible.
    4. En **Período de retención para las grabaciones de vídeo**, defina durante cuánto tiempo desea guardar las grabaciones de vídeo. Puede introducir entre 1 y 999 días, donde 7 días es el periodo de retención predeterminado.
    5. Haga clic en **Continuar**.
7. En la ventana **Seleccionar la ubicación de los archivos y el idioma del producto**, haga lo siguiente:
    1. En el campo **Ubicación del archivo**, seleccione la ubicación donde desee instalar el programa.
    2. En **Idioma del producto**, seleccione el idioma en que quiere instalar su producto XProtect.
    3. Haga clic en **Install** (instalar).

El software se instala.

8. Cuando se haya completado la instalación, aparece una lista de los componentes instalados en el ordenador.

   Haga clic en **Continuar** para añadir hardware y usuarios al sistema.

   Nota: Si hace clic en **Cerrar en este momento**, omitirá el asistente de configuración y se abrirá el XP MC. Puede configurar opciones como, por ejemplo, añadir hardware y usuarios al sistema en el MC.

9. En la ventana **Introducir contraseñas y nombres de usuario para el hardware**, introduzca los nombres de usuario y contraseñas para el hardware que haya modificado de los predeterminados de fábrica.

   El programa de instalación escaneará la red en busca de este hardware, así como para el hardware con credenciales predeterminados de fábrica.

   Haga clic en **Continuar**.

10. En la ventana **Seleccione el hardware que quiere agregar al sistema**, selecciona el hardware que desee añadir al sistema. Haga clic en **Continuar**.

11. En la ventana **Configurar los dispositivos**, puede cambiar el nombre del hardware por uno más útil haciendo clic en el icono de edición junto al nombre del hardware. Este nombre precederá a los dispositivos de hardware.

    Expanda el nodo de hardware para habilitar o deshabilitar dispositivos de hardware como cámaras, altavoces y micrófonos.

    Nota: Las cámaras están habilitadas por defecto, y los altavoces y micrófonos están deshabilitados.

    Haga clic en **Continuar**.

12. En la ventana **Añadir usuarios**, puede añadir usuarios de Windows o usuarios básicos. Estos usuarios pueden cumplir el cometido de Administradores o de Operadores.

    Defina el usuario y haga clic en **Añadir**.

    Cuando haya terminado de añadir usuarios, haga clic en **Continuar**.

Cuando haya completado la instalación y la configuración inicial, aparecerá la ventana **Configuración completada**, donde verá:

- Una lista de las cámaras y dispositivos añadidos a su sistema
- Una lista de los usuarios añadidos a su sistema
- Direcciones al servidor WebCName_XP y Mob_comORbrand, que puede copiar y compartir con sus usuarios

Cuando haga clic en **Cerrar**, el SC_XP se abre y está listo para usar.

Instalar el sistema - Opción de distribución

La opción **Distribuida** instala solo los componentes del servidor de gestión en el equipo actual. Esto significa que el servidor de grabación XProtect Smart Client no está visible en la lista de componentes no modificable. Debe instalar el servidor de grabación, XProtect Smart Client y el servidor SQL en otros equipos.

1. Descargue el software desde Internet (http://www.milestonesys.com/downloads) y ejecute el archivo `Milestone XProtect VMS Products 2018 R2 System Installer.exe` desde la ubicación donde lo guardó.

2. Los archivos de instalación se desempaquetan.En función de la configuración de seguridad, aparecerán una o varias advertencias de seguridad de Windows ®.Acepte estos y el desembalaje continúa.

3. Cuando haya terminado, el cuadro de diálogo **Milestone XProtect VMS** aparece,

    1. Seleccione **Idioma** para usar durante la instalación (esto es **no** el idioma que su sistema utiliza una vez instalado, esto se selecciona más adelante).Haga clic en **Continuar**.

    2. Lea el Milestone Contrato de licencia de usuario final.Seleccione la casilla de verificación **Acepto los términos del contrato de licencia** y haga clic en **Continuar**.

4. En **Escriba o busque la ubicación del archivo de licencia**, ingrese su archivo de licencia de su proveedor de XProtect. Como alternativa, utilice la función de exploración para localizarlo. El sistema verifica el archivo de licencia antes de poder continuar. Haga clic en **Continuar**.Seleccione **Distribuida**. Aparecerá una lista no modificable de los componentes a instalar. Haga clic en **Continuar**.

5. Elija el tipo de base de datos de servidor SQL que quiere. También debe especificar el nombre del servidor SQL. Haga clic en **Continuar**.

6. Seleccione **Crear nueva base de datos** o **Usar base existente** y nombre la base de datos. Si elige la segunda opción, seleccione **Conservar** o **Sobrescribir** los datos existentes. Haga clic en **Continuar**.

7. Selecciones **Ubicación de los archivos** para el archivo del programa. En **Idioma del producto**, seleccione el idioma en que quiere instalar su producto XProtect. Haga clic en **Install** (instalar).

8. El software se instala. Cuando haya terminado, verá una lista de los componentes instalados correctamente. Haga clic en **Cerrar**.

    Microsoft® IIS se instala automáticamente durante el proceso. Después se le pedirá que reinicie el equipo. Hágalo y después de reiniciar, dependiendo de su configuración de seguridad, puede recibir uno o más avisos de seguridad de Windows. Acéptelos y la instalación se completa.

9. Instale como mínimo un servidor de grabación en XProtect Smart Client en otro equipo.

Ver también

Instale el servidor de grabación (en la página 44)

Instale los clientes (ver "Instalar clientes" en la página 51)

Instalar el sistema - Opción de personalización

La opción **Personalizada** instala siempre el servidor de gestión, pero puede seleccionar libremente entre los otros componentes del servidor de gestión, y XProtect Smart Client a instalar en su equipo actual. De manera predeterminada, el servidor de grabación se elimina de la lista de componentes, pero esto se puede modificar. Según su selección, debe instalar los componentes eliminados después en otros equipos además del servidor SQL.

1. Descargue el software desde Internet (http://www.milestonesys.com/downloads) y ejecute el archivo `Milestone XProtect VMS Products 2018 R2 System Installer.exe` desde la ubicación donde lo guardó.

2. Los archivos de instalación se desempaquetan.En función de la configuración de seguridad, aparecerán una o varias advertencias de seguridad de Windows ®.Acepte estos y el desembalaje continúa.

3. Cuando haya terminado, el cuadro de diálogo **Milestone XProtect VMS** aparece,

1. Seleccione **Idioma** para usar durante la instalación (esto es **no** el idioma que su sistema utiliza una vez instalado, esto se selecciona más adelante).Haga clic en **Continuar**.

2. Lea el Milestone Contrato de licencia de usuario final.Seleccione la casilla de verificación **Acepto los términos del contrato de licencia** y haga clic en **Continuar**.

4. En **Escriba o busque la ubicación del archivo de licencia**, ingrese su archivo de licencia de su proveedor de XProtect. Como alternativa, utilice la función de exploración para localizarlo. El sistema verifica el archivo de licencia antes de poder continuar. Haga clic en **Continuar**.Seleccione **Personalizada**. Aparecerá una lista de los componentes a instalar. Aparte del servidor de gestión, todos los demás elementos de la lista son opcionales. El servidor de grabación no está seleccionado de modo predefinido, pero puede seleccionarlo si lo necesita. Haga clic en **Continuar**.

5. Elija el tipo de base de datos de servidor SQL que quiere. Si es relevante, también debe especificar el nombre del servidor SQL. Haga clic en **Continuar**.

6. Seleccione **Crear nueva base de datos** o **Usar base existente** y nombre la base de datos. Si elige la segunda opción, seleccione **Conservar** o **Sobrescribir** los datos existentes. Haga clic en **Continuar**.

7. Seleccione **Esta cuenta predefinida** o **Esta cuenta** para seleccionar la cuenta de servicio. Si es necesario, introduzca una contraseña y confírmela. Haga clic en **Continuar**.

8. Si tiene más de una página Web IIS disponible, puede seleccionar cualquiera de ellas. Sin embargo, si alguna de sus páginas Web posee enlaces HTTPS, seleccione una de ellas. Haga clic en **Continuar**.

9. Selecciones **Ubicación de los archivos** para el archivo del programa. En **Idioma del producto**, seleccione el idioma en que quiere instalar su producto XProtect. Haga clic en **Install** (instalar).

10. El software se instala. Cuando haya terminado, verá una lista de los componentes instalados correctamente. Haga clic en **Cerrar**.

    Microsoft® IIS se instala automáticamente durante el proceso. Después se le pedirá que reinicie el equipo. Hágalo y después de reiniciar, dependiendo de su configuración de seguridad, puede recibir uno o más avisos de seguridad de Windows. Acéptelos y la instalación se completa.

11. Según sus selecciones, instale los servidores restantes en los otros equipos:

    1. Entre en la página de descargas del servidor de gestión desde el menú de **Inicio** de Windows.

    2. Seleccione **Programas** > **Milestone**, **Página de instalación administrativa** y copie la dirección de internet.

    3. Inicie sesión en cada equipo a instalar:

    - Servidor de registro.
    - Servidor de eventos.
    - Management Client.

    1. Abra un navegador de Internet, pegue la dirección de la página de descargas de los servidores de gestión en el campo de dirección y descargue el instalador adecuado.

    2. Ejecute el instalador.

12. Instale el servidor de grabación en un equipo separado, consulte Instalar el servidor de grabación (ver "Instale el servidor de grabación" en la página 44).

Instale el servidor de grabación

Una vez que haya instalado el servidor de gestión, descargue el instalador del servidor de grabación independiente del administrador de descargas del servidor de administración.

El servidor de grabación está autorizado automáticamente a trabajar con el servidor de gestión después de ejecutar el instalador del servidor de grabación.

Nota: El servidor de grabación ya está instalado cuando se realiza una instalación **Único equipo**.

Ver Instalar un servidor de grabación failover (en la página 104) si desea instalar un servidor failover.

Para acceder a la página web de instalación:

1. Inicie sesión en el equipo en el que desea instalar el servidor de grabación y abra un navegador de Internet.
2. Ingrese la siguiente URL en su navegador: http://[dirección del servidor de gestión]/installation/admin

   [management server address] es la dirección IP o nombre de host del servidor de gestión.
3. Seleccione **Todos los idiomas** debajo del **instalador del servidor de grabación**. Guarde el instalador en algún lugar apropiadamente y ejecútelo desde aquí o ejecútelo directamente desde la página web.
4. Seleccione el **Idioma** que desea utilizar durante la instalación. Haga clic en Continuar.
5. Seleccionar:

   Típico: para instalar un servidor de grabación con valores predeterminados o

   Personalizado: para instalar un servidor de grabación con valores personalizados.
6. Especificar la configuración del servidor de grabación:
   - **Nombre**
   - **Dirección del servidor de gestión**
   - **Ruta** para guardar grabaciones y haga clic en **Continuar**.
7. Si ha seleccionado **Personalizado**:
   1. Especifique la cantidad de servidores de grabación que desea instalar en esta computadora. Haga clic en **Continuar**.
   2. Especificar la cuenta de servicio. Si es necesario, introduzca una contraseña y confirmar esto. Haga clic en **Continuar**.
8. Seleccione **Ubicación de los archivos** para el archivo de programa. En **Idioma del producto**, seleccione el idioma en el que desea instalar su sistema. Haga clic en **Install (instalar)**.
9. El software ahora está instalado. Una vez que se completa, verá una lista de componentes instalados correctamente. Haga clic en **Cerrar**.

   Cuando haya instalado el servidor de grabación, puede verificar su estado desde el icono de la bandeja del Recording Server Manager.
10. Cuando haya terminado, la instalación se completa y puede continuar con la configuración. Consulte Proceso de configuración (ver "Configure el sistema en el Management Client" en la página 49).

Instalar un servidor de grabación en silencio

La ventaja de una instalación silenciosa es que se puede hacer de forma remota. Siga los pasos a continuación:

1. Busque el archivo de instalación del servidor de grabación: MilestoneXProtectRecordingServerInstaller_x64.exe.

    1. Iniciar sesión en el servidor de gestión.
    2. Abra un navegador de Internet y escriba la dirección: http://localhost/Installation/Admin/
    3. Guarde el archivo de instalación del servidor de grabación en el servidor donde desea instalar el nuevo servidor de grabación.

    O puede buscar el archivo. La ruta suele ser: C:\Program Files\Milestone\XProtect Management Server\IIS\httpdocs\Admin\Recording Server Installer\[version number] [bit-version]\All Languages\en-US

2. Ejecute una instalación silenciosa con la configuración de parámetros predeterminada:

    Para ejecutar una instalación silenciosa utilizando los valores por defecto para todos los parámetros, inicie un símbolo del sistema (cmd. exe) en el directorio donde se encuentra el programa de instalación y realizar comando siguiente:

    MilestoneXProtectRecordingServerInstaller_x64.exe --quiet

3. O haga una instalación personalizada. Debe especificar los parámetros que desea sobrescribir:

    Por ejemplo, para cambiar la ruta de acceso al servidor de gestión de la instalación, ejecute:

    MilestoneXProtectRecordingServerInstaller_x64.exe --quiet --parameters=SERVERHOSTNAME:DKWS-OKR-02

    Estos son los parámetros que se pueden utilizar a través de parámetros de línea de comandos:

    - Para cambiar el nombre del servidor de grabación:

        RECORDERNAME - nombre de la grabadora que aparecerá en el Management Client.

        --quiet --parameters=RECORDERNAME:NewRecorderName

    - Para instalar el servidor de grabación como failover:

        ISFAILOVER - establecer este indicador en True

        --quiet --parameters=ISFAILOVER:True

    - Para cambiar servidor de gestión:

        SERVERHOSTNAME - nombre de host del servidor de gestión de servidor de grabación, donde se conectará a

        SERVERPORT - puerto del servidor de gestión (80 por defecto)

        --quiet --parameters=SERVERHOSTNAME:DKWS-OKR-02

    - Para instalar Recording Server como usuario diferente de NT AUTHORITY\NETWORK SERVICE:

        RECUSERACCOUNT - bandera que determina si se utiliza la cuenta de usuario o una de las cuentas predefinidas

RECSERVICEACCOUNT - nombre del usuario utilizado o cuenta de servicio predefinida

- Con el fin de cambiar la ubicación de la instalación de forma predeterminada en primer lugar debe realizar:

  MilestoneXProtectRecordingServerInstaller_x64.exe --generateargsfile=C:\temp

  En la ubicación especificada se encuentra el archivo . xml con los parámetros. Por lo que sería necesario cambiar los parámetros en este archivo y ejecutar la instalación con el archivo recién modificado.

- Para cambiar la ubicación de la instalación:

  INSTALLDIR - camino en el servidor de grabación debe estar instalado para

  TARGETDIR - debe ser el mismo que INSTALLDIR

  INSTALLLOCATION - debe ser el mismo que INSTALLDIR

- Para cambiar la ubicación de las grabaciones:

  MEDIADBPATH - ruta de acceso a la base de datos multimedia con todas las grabaciones

  Por ejemplo modificaciones en mi Argements. xml eran. Mi nueva ubicación de la instalación estará %ProgramFiles(x86)%\Milestone\ y nueva ubicación para las grabaciones es C:\MD

  <KeyValueParametersOfStringString>

  <Value>**%ProgramFiles(x86)%\Milestone\bla**</Value>

  <Key>INSTALLDIR</Key>

  </KeyValueParametersOfStringString>

  <KeyValueParametersOfStringString>

  <Value>**%ProgramFiles(x86)%\Milestone\bla**</Value>

  <Key>TARGETDIR</Key>

  </KeyValueParametersOfStringString>

  <KeyValueParametersOfStringString>

  <Value>**%ProgramFiles(x86)%\Milestone\bla**</Value>

  <Key>INSTALLLOCATION</Key>

  </KeyValueParametersOfStringString>

  <KeyValueParametersOfStringString>

  <Value>**C:\MD**</Value>

  <Key>**MEDIADBPATH**</Key>

  </KeyValueParametersOfStringString>

  Corre el:

MilestoneXProtectRecordingServerInstaller_x64.exe --quiet --arguments=C:\temp\Arguments_.xml

Solución de problemas

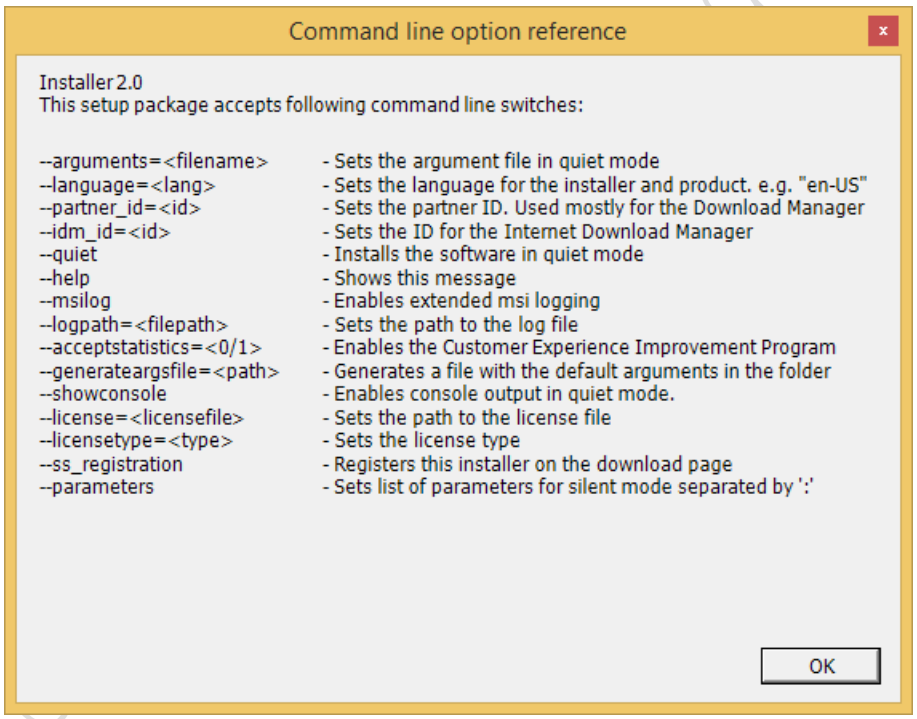
¿Dónde puedo encontrar los archivos de registro de la instalación?
Los archivos de registro de la instalación se encuentran debajo **C:\ProgramData\Milestone\Installer**

¿Cómo veo una lista de parámetros predeterminados que se utilizarán durante una instalación de Único equipo?
Para ver una lista de parámetros con todos los valores por defecto puede ejecutar **MilestoneXProtectRecordingServerInstaller_x64.exe --generateargsfile=C:\temp**

Se generará un archivo llamado Arguments. xml en la carpeta especificada.

¿Cómo puedo ver los parámetros que se utilizaron durante la instalación de medida?
La lista completa de los parámetros utilizados para ejecutar la instalación están en **C:\ProgramData\Milestone\Installer\Milestone XProtect Recording Server (64_bit)I.log** + búsqueda de la "línea de comandos"/"Command line"

¿Cómo puedo ver una lista completa de los posibles parámetros?
Ejecutar **MilestoneXProtectRecordingServerInstaller_x64. exe --help**



Configurar la autenticación Kerberos

Utilizar la autenticación Kerberos como una alternativa al protocolo de autenticación anteriores Microsoft NT LAN (NTLM).

Consulte Autenticación Kerberos (explicada) (en la página 34) para obtener más información.

Instalación de grupos de trabajo

Si no usa una configuración de dominio con un servidor Active Directory y usa un grupo de trabajo, siga los siguientes pasos:

1. Inicie sesión en Windows con una cuenta de administrador común.

   Asegúrese de usar la misma cuenta en todos los equipos del sistema.

2. Según sus necesidades, puede iniciar la instalación del servidor de gestión o de grabación y haga clic en **Personalizada**.

3. Según lo que ha seleccionado en el paso 2, seleccione instalar el servicio de Management o Recording Server usando una cuenta de administrador común.

4. Complete la instalación.

5. Repita los pasos 1-4 para instalar cualquier otro sistema que quiera conectar. Todos deben ser instalados usando una cuenta de administrador común.

No puede usar este método cuando **actualice** las instalaciones de grupos de trabajo. Consulte Actualización alternativa para grupo de trabajo (ver "Actualización alternativa para el grupo de trabajo" en la página 61).

Solución de problemas de instalación

Los siguientes problemas pueden ocurrir durante o después de la instalación de los servidores del servidor de gestión o de grabación. Para cada tema, una o más soluciones están disponibles.

Problema: Grabación de inicio del servidor falla debido a conflicto de puertos

Este problema sólo puede aparecer si se ejecuta el servicio Simple Mail Transfer Protocol **(** SMTP) ya que utiliza el puerto 25. Si el puerto 25 ya está en uso, puede que no sea posible iniciar el servicio de servidor de grabación. Es importante que el número de puerto 25 está disponible para el servicio SMTP del servidor de grabación.

Servicio SMTP: Verificación y soluciones

Para comprobar si está instalado el servicio SMTP:

1. Desde el menú **Inicio** de Windows, seleccione **Panel de control**.

2. En el **Panel de control**, haga doble clic en **Añadir o quitar programas**.

3. En la parte izquierda de la ventana de **Añadir o quitar programas**, haga clic en **Añadir o quitar componentes de Windows**.

4. En el asistente para **componentes de Windows**, seleccione **Internet Information Server (IIS)**, y haga clic en **Detalles**.

5. En la ventana de **Internet Information Services (IIS)**, compruebe si la casilla de verificación **SMTP Service** está seleccionada. Si es así, el Servicio SMTP está instalado.

Si el Servicio SMTP está instalado, pruebe con una de las siguientes soluciones:

Solución 1: Deshabilite el Servicio SMTP, o active el inicio manual

Esta solución le permite iniciar el servidor de grabación sin tener que detener el Servicio SMTP cada vez:

1. Desde el menú **Inicio** de Windows, seleccione **Panel de control**.

2. En el **Panel de control**, haga doble clic en **Herramientas administrativas**.
3. En la ventana de **Herramientas administrativas**, haga doble clic en **Servicios**.
4. En la ventana de **Servicios**, haga doble clic en **Protocolo simple de transferencia de correo (SMTP)**.
5. En la ventana **Propiedades SMTP**, haga clic en **Detener**, a continuación, establezca el **tipo de inicio** ya sea **manual** o **Deshabilitado**.

   Cuando está en **Manual**, el Servicio SMTP puede iniciarse manualmente desde la ventana de **Servicios**, o desde una ventana de interfaz del sistema utilizando el comando net start SMTPSVC.
6. **Haga clic en OK (aceptar)**.

Solución 2: Eliminar el servicio SMTP

Extracción del servicio SMTP puede afectar a otras aplicaciones que utilizan el servicio SMTP.

1. Desde el menú **Inicio** de Windows, seleccione **Panel de control**.
2. En la ventana **Panel de control**, haga doble clic **Añadir o quitar programas**.
3. En la parte izquierda de la ventana de **Añadir o quitar programas**, haga clic en **Añadir o quitar componentes de Windows**.
4. En el Asistente para **componentes de Windows**, seleccione elemento **Internet Information Server (IIS)** y haga clic **detalles**.
5. En la ventana de Servicios de **Internet Information Services (IIS)**, desmarque la casilla del **Servicio SMTP**.
6. Haga clic en **Aceptar**, **Siguiente** y **Finalizar**.

Problema: Los cambios en la ubicación del SQL Server impiden el acceso a la base de datos

Este es un problema si se cambia la ubicación del servidor SQL Server, por ejemplo, cambiando el nombre de host del equipo que ejecuta el servidor SQL Server. El resultado de este problema es que el acceso a la base de datos se pierde.

Solución: Utilice la herramienta de actualización de la dirección SQL que se encuentra en el icono de la bandeja del Recording Server Manager.

Configure el sistema en el Management Client

A continuación, se muestra una lista de las tareas típicas para configurar el sistema.

Incluso si las tareas se listan como una lista de verificación, una lista de verificación completa no garantiza por sí misma que el sistema coincida con los requisitos exactos de su organización. Para que el sistema coincida con las necesidades de su organización, Milestone recomienda que supervise y ajuste el sistema continuamente.

Por ejemplo, es una buena idea probar y ajustar los ajustes de sensibilidad de detección de movimiento de cámaras individuales bajo diferentes condiciones físicas, incluyendo día / noche y clima ventoso, una vez que el sistema esté funcionando.

La configuración de reglas, que determinan la mayoría de las acciones que realiza su sistema, incluyendo cuándo grabar vídeo, es otro ejemplo de configuración que puede cambiar de acuerdo con las necesidades de su organización.

☑	Ha finalizado la instalación inicial de su sistema. Ver Instale el sistema (en la página 37).
☑	Cambie el SLC de prueba a un SLC permanente (si es necesario). Ver Código de licencia de software de cambio (ver "Cambiar el código de licencia de software" en la página 51).
☑	Inicie sesión en el Management Client.
☐	Verifique que las configuraciones de almacenamiento de cada servidor de grabación satisfagan sus necesidades. Ver Almacenamiento y archivo (explicado) (en la página 82).
☐	Compruebe que la configuración de archivado de cada servidor de grabación responda a sus necesidades. Consulte Propiedades de configuración de archivo (ver "Propiedades Configuración de archivo" en la página 93).
☐	Detectar el hardware, cámaras o codificadores de vídeo para agregar a cada servidor de grabación. Ver Agregar hardware (ver "Añadir hardware" en la página 109).
☐	Configure las cámaras individuales de cada servidor de grabación. Ver Dispositivos de cámara (explicado) (en la página 123).
☐	Permite el almacenamiento y el archivado de cámaras individuales o de un grupo de cámaras. Esto se hace desde las cámaras individuales o desde el grupo de dispositivos. Consulte Adjuntar un dispositivo o grupo de dispositivos a un almacenamiento (ver "Conectar un dispositivo o grupo de dispositivos a un almacenamiento" en la página 86).
☐	Habilitar y configurar dispositivos. Ver Trabajar con dispositivos (en la página 123).
☐	Las reglas determinan el comportamiento del sistema en gran medida. Crea reglas para definir cuándo deben grabar las cámaras, cuando las cámaras de zoom panorámico (PTZ) deben patrullar y cuando se deben enviar notificaciones, por ejemplo. Crear reglas. Ver Reglas y eventos (explicado) (en la página 184).
☐	Agrega cometidos al sistema. Ver Cometidos (explicado) (ver "Cometidos (explicados)" en la página 228).
☐	Agregue usuarios y / o grupos de usuarios a cada una de los cometidos. Ver Asignar / eliminar usuarios y grupos de / a los cometidos (ver "Asignar / eliminar usuarios y grupos a / desde los cometidos" en la página 231).
☐	Activar licencias. Ver Activar licencias en línea (en la página 76) o Activar licencias sin conexión (ver "Activar las licencias en línea" en la página 76).

Cambiar el código de licencia de software

Si ejecuta la instalación con un código de licencia de software de prueba durante el primer periodo, puede cambiarlo a un SLC permanente sin tener que volver a instalar el sistema.

Importante: Esto se debe realizar localmente desde el servidor de gestión. **No** se puede hacer desde Management Client.

1. En el servidor de gestión, entre en el área de notificación de la barra de tareas.

2. Haga clic con el botón derecho en el icono del **servidor de gestión** y seleccione **Cambiar licencia**.
3. Haga clic en **Importar licencia**.
4. A continuación, seleccione el archivo de licencia SLC guardado con este propósito. Cuando lo haga, se añade la ubicación del archivo de licencia seleccionado justo debajo del botón **Importar licencia**.
5. Haga clic en **Aceptar** y ya puede registrar el SLC. Consulte Registrar SLC (ver "Registrar el código de licencia de software" en la página 36).

Rangos de direcciones IP locales (explicados)

Cuando un cliente, como XProtect Smart Client, se conecta a un sistema de vigilancia, una cantidad de la comunicación inicial de datos, incluido el intercambio de direcciones de contacto que pasa en el fondo. Esto sucede automáticamente, y es transparente para los usuarios.

Los clientes pueden conectarse desde la red local, así como a través de Internet, y en cada caso el sistema de vigilancia debe ser capaz de proporcionar las direcciones adecuadas de modo que los clientes pueden acceder a video en directo y grabado desde los servidores de grabación:

- Cuando los clientes se conectan a nivel local, el sistema de vigilancia debe responder con las direcciones locales y números de puerto.
- Cuando los clientes se conectan a través de Internet, el sistema de vigilancia debe responder con direcciones públicas de los servidores de grabación, es decir, la dirección del firewall o router NAT (Network Address Translation), ya menudo también un número de puerto diferente (que luego se transmitió a la grabación servidores).

Por consiguiente, el sistema de vigilancia debe ser capaz de determinar si un cliente pertenece en un rango de IP local o en Internet. Para este propósito, se puede definir una lista de rangos de IP, que el sistema de vigilancia debe reconocer como procedentes de una red local.

Instalar clientes

Instalar XProtect Smart Client en modo silencioso

Puede implementar XProtect Smart Client o su software de vigilancia en los ordenadores de los usuarios mediante herramientas como Microsoft Systems Management Server (SMS). Este tipo de herramientas le permite crear bases de datos de hardware y software en las redes locales. Posteriormente, las bases de datos

se pueden usar, entre otras cosas, para distribuir e instalar aplicaciones de software, como XProtect Smart Client, a través de redes locales.

1. Busque el archivo del programa de instalación (.exe) de Smart Client; (XProtect Smart Client 2018 R2 Installer.exe o XProtect Smart Client 2018 R2 Installer x64.exe) para las versiones de 32 bits y 64 bits respectivamente. Encontrará el archivo en una subcarpeta de la carpeta **httpdocs**. La carpeta **httpdocs** está ubicada como subcarpeta en la que su software de vigilancia Milestone está instalado.

   Normalmente la ruta es:
   C:\Archivos de programa\Milestone\XProtect Management Server\IIS\httpdocs\XProtect Smart Client Installer\[número de versión] [bit-version]\All Languages\en-US

   Por ejemplo:
   C:\Archivos de programa\Milestone\XProtect Management Server\IIS\httpdocs\XProtect Smart Client Installer\2018 R1 (32-bit)\All Languages\en-US

2. Ejecute una instalación silenciosa utilizando una de las siguientes dos opciones:

   - Ejecutar con ajustes de parámetros por defecto:

     Para ejecutar una instalación silenciosa utilizando los valores por defecto para todos los parámetros, abra una ventana de comandos (cmd.exe) en el directorio en el que se encuentre el programa de instalación y ejecute el siguiente comando:

     XProtect Smart Client 2018 R2 Installer.exe --quiet

     Esto ejecuta una instalación silenciosa de XProtect Smart Client utilizando valores por defecto para parámetros como el directorio de destino, etc. Para cambiar los ajustes por defecto, véase a continuación.

   - Personalizar parámetros por defecto utilizando un archivo de argumento xml como entrada:

     Para personalizar los ajustes de instalación por defecto, incluya un archivo xml con valores modificados como entrada. Para generar el archivo xml con valores por defecto, abra una ventana de comandos en el directorio en el que se encuentre el programa de instalación y ejecute el siguiente comando:

     XProtect Smart Client 2018 R2 Installer.exe --generateargsfile=[path]

     Abra el archivo Arguments.xml generado, utilizando por ejemplo el Bloc de notas de Windows, y realice los cambios necesarios. A continuación, para ejecutar la instalación silenciosa utilizando estos valores modificados, ejecute el siguiente comando en el mismo directorio.

     XProtect Smart Client 2018 R2 Installer.exe --arguments=args.xml --quiet

Instalar el servidor Milestone Mobile

Una vez que haya instalado el servidor Milestone Mobile, puede utilizar Milestone Mobile y XProtect Web Client con su sistema. Para reducir el uso total de recursos del sistema en el equipo que ejecuta el servidor de gestión, instale el servidor Milestone Mobile en un equipo independiente.

El servidor de gestión tiene una página web pública de instalación incorporado. A partir de esta página web, los administradores y usuarios finales pueden descargar e instalar los componentes del sistema XProtect necesarios desde el servidor de gestión o cualquier otro ordenador en el sistema.

Para acceder a la página web de instalación:

1. Introduzca la siguiente URL en el navegador: http://[management server address]/installation/admin

[management server address] es la dirección IP o nombre de host del servidor de gestión.

2. Haga clic en **Todos los idiomas** para el instalador Milestone Mobile.
3. Ejecutar el archivo descargado. Haga clic en **Sí** en todas las advertencias. Comienza la descompresión.
4. Elija un idioma para el instalador. Haga clic en **Continuar**.
5. Lea y acepte el contrato de licencia. Haga clic en **Continuar**.
6. Seleccionar el tipo de instalación.
   - Haga clic en **Típico** para instalar el servidor y el complemento Milestone Mobile.
   - **Personalizado** - Instale sólo el servidor o sólo el complemento. Por ejemplo, instalar solo el plug-in es útil cuando quiere usar Management Client para gestionar servidores Milestone Mobile, pero no necesita el servidor Milestone Mobile en ese equipo.

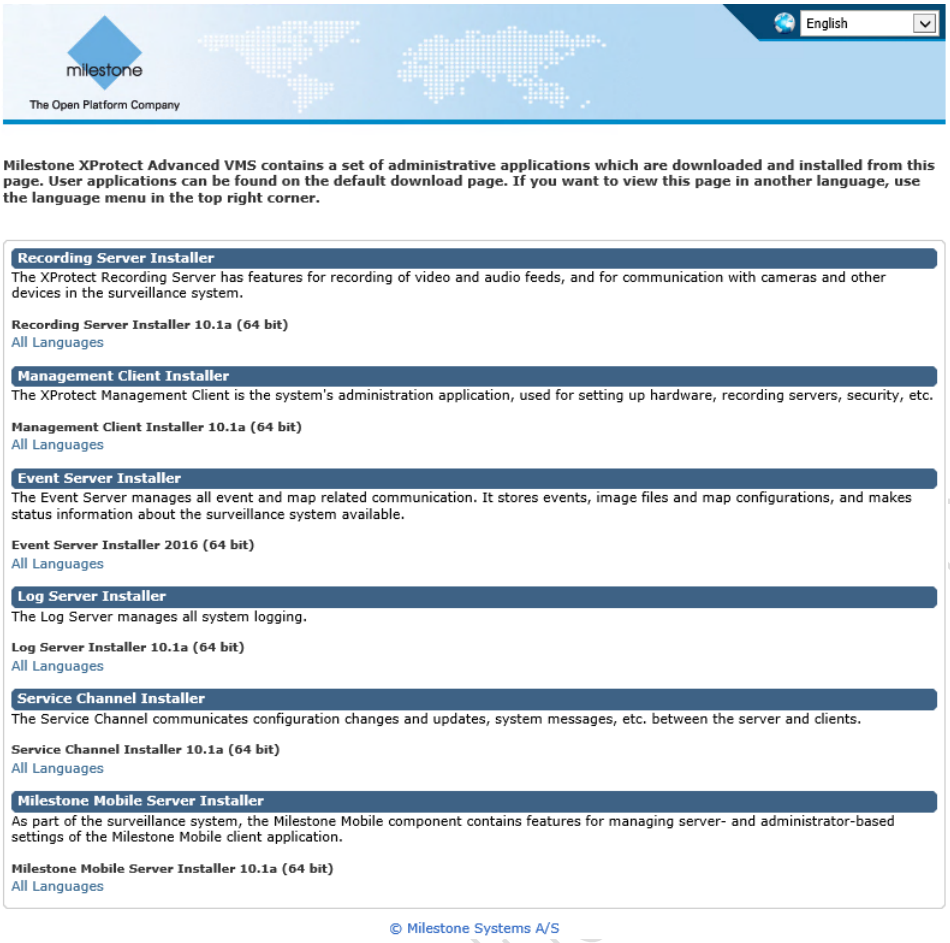
   El complemento Milestone Mobile es necesario en el equipo que ejecuta Management Client para administrar servidores Milestone Mobile en Management Client.

   El complemento Milestone Mobile es una parte común de la instalación Management Client, pero la instalación del complemento es necesaria cuando desea actualizar el complemento.
7. Introduzca la siguiente información sobre el servidor del sistema de vigilancia primario:
   - URL de servidor de gestión
   - Iniciar sesión
   - Nombre de usuario y contraseña. Haga clic en **Continuar**.
8. Seleccione la ubicación del archivo y el idioma del producto y haga clic en **Instalar**.
9. Cuando se completa la instalación, aparece una lista de componentes instalados correctamente. Haga clic en **Cerrar**.

Usted está listo para configuración del Milestone Mobile (ver "Configuración Milestone Mobile" en la página 389).

Download Manager/página Web de descargas

El servidor de gestión incorpora una página web. La página web permite a los administradores y usuarios finales descargarse e instalar los componentes necesarios del sistema XProtect de vigilancia desde cualquier lugar, de forma local o remota.



La página Web puede mostrar dos grupos de contenido, ambos de manera predeterminada en el idioma de la instalación del sistema:

- una página web está dirigida a **administradores**, permitiendo descargar e instalar los componentes claves del sistema. En la mayoría de casos la página Web se carga automáticamente al concluir la instalación del servidor de gestión y se muestra el contenido predeterminado. En el servidor de gestión, puede acceder a la página web desde el menú de **Inicio** de Windows, seleccione **Programas**> **Milestone** > **Página de instalación administrativa**. También puede introducir el enlace:

  http://[dirección servidor de gestión]:[puerto]/installation/admin/

  [dirección servidor de gestión] es la dirección IP o nombre de host del servidor de gestión y [puerto] es el número de puerto en el que ha configurado IIS para usar en el servidor de gestión. Si no consigue acceder a la página web del servidor de gestión, inicie sesión con una cuenta que tenga derechos de administración sobre el servidor de gestión.

- Otra página web dirigida a **usuarios finales**, que proporciona acceso a las aplicaciones del cliente con la configuración predeterminada. En el servidor de gestión, puede acceder a la página web desde el menú de **Inicio** de Windows, seleccione **Programas**> **Milestone** > **Página de instalación pública**. También puede introducir el enlace:

  http://[dirección servidor de gestión]:[puerto]/installation/

  [dirección servidor de gestión] es la dirección IP o nombre de host del servidor de gestión y [puerto] es el número de puerto en el que ha configurado IIS para usar en el servidor de gestión.

Las dos páginas Web poseen contenido predeterminado para que se puedan usar directamente después de la instalación. Sin embargo, como administrador, al usar Download Manager, puede personalizar lo que se debe

visualizar en las páginas Web. También puede mover los componentes entre las dos versiones de la página web. Para mover un componente, haga clic con el botón secundario y seleccionar la versión de la página web a la que quiere mover el componente.

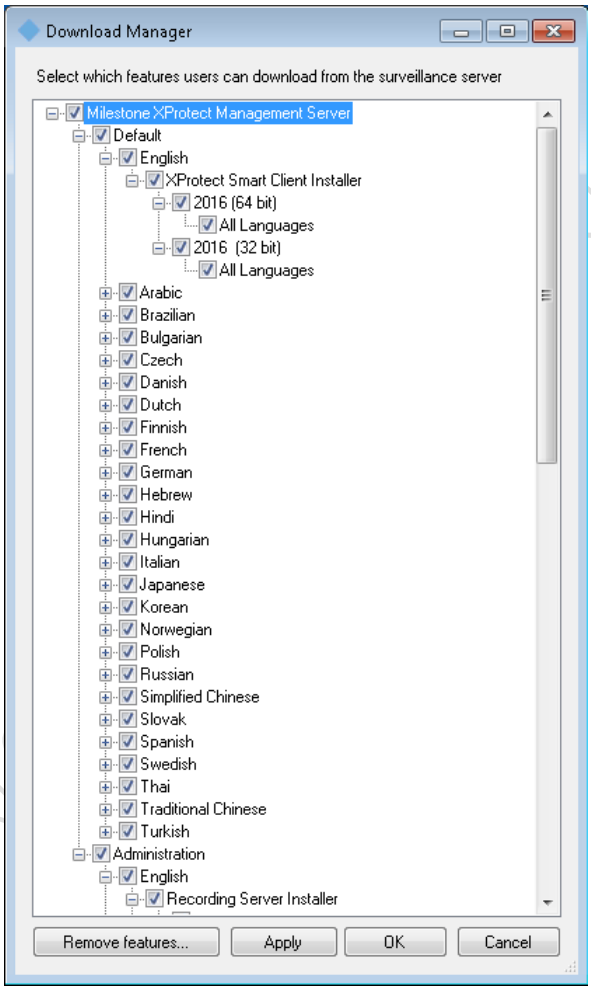
A pesar de que puede controlar qué componentes pueden descargar e instalar los usuarios en Download Manager, no puede usarlo como una herramienta de gestión de derechos de usuario. Esos derechos los determinan los cometidos definidos en Management Client.

En el servidor de gestión, puede acceder a XProtect Download Manager desde el menú de **Inicio** de Windows, seleccione **Programas** > **Milestone** > **XProtect Gestor de descargas**.

Configuración predeterminada de Download Manager

El Download Manager tiene una configuración por defecto. Esto asegura que los usuarios de su organización pueden tener acceso a los componentes estándar desde el principio.

La configuración por defecto que proporciona una configuración por defecto con el acceso a la descarga de componentes adicionales u opcionales. Por lo general, se accede a la página web desde el ordenador servidor de gestión, pero también se puede acceder a la página web desde otros ordenadores.



- El primer nivel: Se refiere a su producto XProtect.
- El segundo nivel: Se refiere a las dos versiones específicas de la página web. **Por defecto** hace referencia a la versión de la página web vista por los usuarios finales. **Administración** se refiere a la versión de página Web vistos por los administradores del sistema.

- El tercer nivel: Se refiere a los idiomas en los que la página web está disponible.
- El cuarto nivel: Se refiere a los componentes que son - o se pueden hacer - disposición de los usuarios.
- El quinto nivel: Se refiere a las versiones particulares de cada componente, que son - o - se pueden hacer disponibles a los usuarios.
- El sexto nivel: Se refiere a las versiones lingüísticas de los componentes que son - o - se pueden hacer disponibles a los usuarios.

El hecho de que sólo los componentes estándar están disponibles inicialmente - y sólo en la misma versión de idioma que el sistema en sí mismo - ayuda a reducir el tiempo de instalación y ahorrar espacio en el servidor. No hay necesidad de tener una versión del componente o de los idiomas disponibles en el servidor si nadie lo utiliza.

Usted puede hacer más componentes o idiomas disponibles según sea necesario y puede ocultar o eliminar los componentes no deseados o idiomas.

Instaladores estándar de Download Manager (usuario)

De manera predeterminada, los siguientes componentes están disponibles para ser instalados independientemente desde la página de descargas del servidor de gestión dirigida a los usuarios (controlada por Download Manager):

- Grabación de servidores, incluyendo servidores de grabación failover. Servidores de grabación failover se descargan e instalan inicialmente como servidores de grabación, durante el proceso de instalación se especifica que desea que un servidor de grabación failover.
- Management Client
- XProtect Smart Client
- Servidor de eventos, usado en conexión con el mapa de funcionalidad
- Servidor de registros, usado para proporcionar la funcionalidad necesaria para la información del sistema de registro
- Canal de servicio, permite la comunicación de configuración automática y transparente entre los servidores y los clientes.
- Milestone Mobile servidor - **solamente disponible aquí**
- Puede haber más opciones disponibles en su organización.

Para la instalación de **paquetes de dispositivos**, véase el instalador de paquete de de dispositivos - debe ser descargado (ver "Instalador de paquete de dispositivos - debe ser descargado" en la página 58).

Componentes del instalador de Añadir/Publicar Download Manager

Usted debe completar dos procedimientos para hacer que los componentes no estándar y las nuevas versiones disponibles en la página de descargas del servidor de gestión.

Primero usted **agrega componentes nuevos y / o no estándar a la Download Manager**. Después debe utilizarlo para **establecer qué componentes distribuir** en las distintas versiones en otros idiomas de la página web.

Si el Download Manager está abierta, cerrarla antes de instalar nuevos componentes.

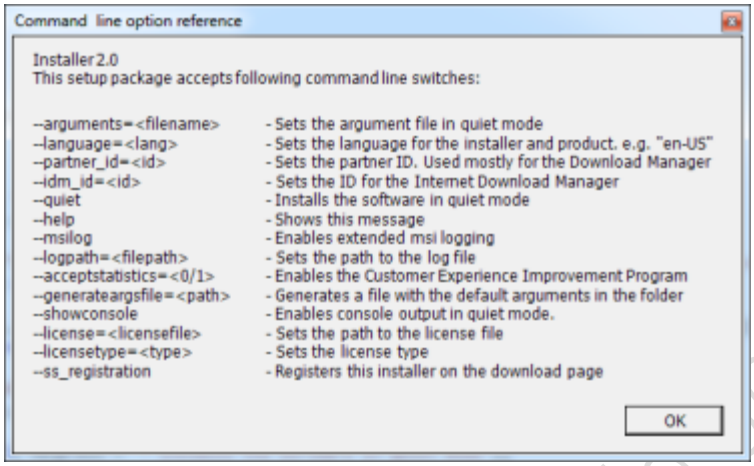
Añadir archivos nuevos/no habituales a Download Manager:

1. En el equipo donde se ha descargado el componente (s), ir a la ventana de **inicio**, introduzca un símbolo del Comando
2. En el símbolo del sistema, ejecute el nombre del archivo (.exe) con: [espacio] --ss_registration

   Ejemplo: RecordingServer_setup_x64.exe --ss_registration

   Ahora, el archivo se añade al Download Manager, pero **no** instalado en el equipo actual.

Para obtener una visión general de los comandos del instalador, en el símbolo del sistema, escribe [espacio] --help y la siguiente ventana aparece:



Cuando se ha instalado nuevos componentes que son por defecto seleccionado en el Download Manager y están inmediatamente disponibles para los usuarios a través de la página web. Siempre puede mostrar y ocultar características en la página web seleccionando o desmarcando las casillas de la estructura de árbol de Download Manager.

Puede cambiar la secuencia en la que se muestran los componentes en la página web. En la estructura de árbol del gestor de Download Manager, arrastre los componentes hasta la posición deseada.

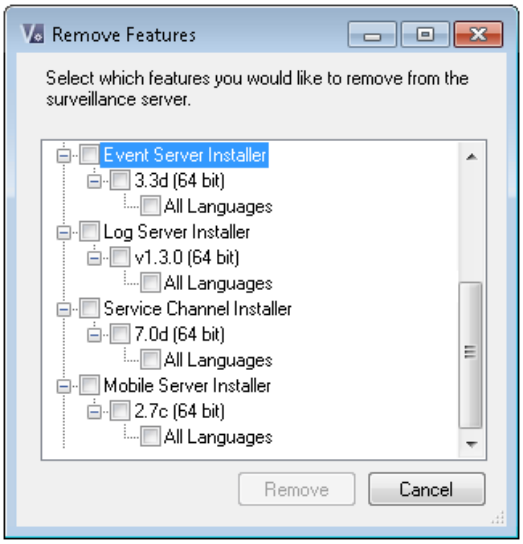
Ocultar / eliminar componentes del instalador Download Manager

Tiene tres opciones:

- **Ocultar componentes** de la página web desactivando casillas de verificación en la estructura de árbol de Download Manager. Los componentes siguen instalados en el servidor de gestión, y mediante la selección de las casillas de verificación en la estructura de árbol de Download Manager se puede hacer rápidamente los componentes disponibles de nuevo.
- **Elimine la instalación de los componentes** en el servidor de gestión. Los componentes desaparecen del Download Manager, pero los archivos de instalación de los componentes se mantienen en C:\Program Files (x86)\Milestone\XProtect Download Manager, para que pueda volver a instalarlos más tarde si es necesario.

  1. En el Download Manager, haga clic en **Quitar características**.

2. En el **Eliminar funciones** ventana, seleccione la característica(s) que desea eliminar.



3. Haga clic en **OK** y **Sí**.

- **Elimine los archivos de instalación de las funciones no requeridas** del servidor de gestión. Esto puede ayudar a ahorrar espacio en disco en el servidor si sabe que su organización no va a utilizar ciertas funciones.

Instalador de paquete de dispositivos - debe ser descargado

El paquete de dispositivo (que contiene los controladores de dispositivo) incluido en su instalación original no está incluido en el Download Manager. Por lo tanto, si necesita volver a instalar el paquete de dispositivos o hacer que el instalador del paquete de dispositivos disponibles, primero debe añadir o publicar el último instalador de paquete de dispositivos para el Download Manager:

1. Obtenga el último paquete de dispositivo regular de la página de descarga en el sitio web (http://www.milestonesys.com/downloads) Milestone.

2. En la misma página, puede descargar el paquete de dispositivo heredado con controladores anteriores. Para verificar si sus cámaras usan controladores del paquete de dispositivo heredado, vaya al https://www.milestonesys.com/community/business-partner-tools/device-packs/ (https://www.milestonesys.com/community/business-partner-tools/device-packs/).

3. Añadir / publicarlo en el Download Manager llamando con el comando --ss_registration.

Si usted no tiene una conexión de red, puede volver a instalar todo el servidor de grabación desde el Download Manager. Los archivos de instalación para el servidor de grabación se ubican localmente en su computadora y de esta manera, automáticamente se vuelve a instalar el paquete de dispositivos.

Actualizar

Actualización (explicado)

Importante: Su sistema XProtect ya no soporta Microsoft Windows XP.

Cuando se actualiza, todos los componentes, excepto la base de datos del servidor de gestión, se eliminan y sustituyen automáticamente. Esto incluye los controladores de su paquete de dispositivo .

La base de datos del servidor de gestión contiene toda la configuración del sistema (configuraciones de servidor de grabación , las configuraciones de las cámaras, reglas, y así sucesivamente). Mientras no se quita la base de datos del servidor de gestión, no es necesaria ninguna reconfiguración de la configuración del sistema, aunque es posible que desee configurar algunas de las nuevas características de la nueva versión.

Nota: La compatibilidad con servidores de grabación de versiones XProtect anteriores de esta versión actual es limitada. Todavía puede acceder a grabaciones en servidores de grabación más antiguos, pero para poder cambiar su configuración, deben ser de la misma versión que la actual. Milestone recomienda que actualice todos los servidores de grabación en su sistema.

Cuando actualice incluyendo sus servidores de grabación, se le preguntará si desea **actualizar** o **mantener** sus controladores de dispositivo de video. Si decide actualizar, sus dispositivos de hardware pueden tardar unos minutos en conectarse a los nuevos controladores de dispositivos de video después de reiniciar su sistema. Esto se debe a varias comprobaciones internas en los controladores recién instalados.

Importante: Si actualiza desde la versión 2017 R3 o anterior a la versión 2018 R1 o posterior, y si su sistema tiene cámaras anteriores, debe descargar manualmente el paquete del dispositivo con controladores heredados desde la página de descarga en nuestro sitio web (http://www.milestonesys.com/downloads). Para ver si tiene cámaras que usan controladores en el paquete de dispositivo heredado, visite esta página en nuestro sitio web (https://www.milestonesys.com/community/business-partner-tools/device-packs/).

Importante: Si actualiza desde la versión 2018 R1 o anterior a la versión 2018 R2 o posterior, es importante que actualice todos los servidores de grabación en su sistema con un parche de seguridad antes de realizar la actualización. La actualización sin el parche de seguridad hará que fallen los servidores de grabación.

Las instrucciones para instalar el parche de seguridad en sus servidores de grabación están disponibles en nuestro sitio web (https://www.milestonesys.com/security-patch-remoting).

Requisitos de actualización

- Tiene su **archivo de licencia de software** (ver "**Licencias (explicadas)**" en la página 23) (.lic) listo.
  - **Actualización del Service Pack**; Durante la instalación del servidor de gestión, el asistente puede pedirle que especifique la ubicación del archivo de licencia de software. Se puede utilizar tanto el archivo de licencia de software que recibió después de la compra de su sistema (o la última actualización) y el archivo de licencia de software activado que recibió después de su última activación de la licencia.
  - **Actualización de versión:** Después de adquirir la nueva versión, se recibe un nuevo archivo de licencia de software. Durante la instalación del servidor de gestión, el asistente le pide que especifique la ubicación del nuevo archivo de licencia de software.

El sistema verifica el archivo de licencia de software antes de poder continuar. Dispositivos de hardware ya se han agregado y otros dispositivos, que requieren licencias entran en un período de gracia. Si no ha activado la activación automática de la licencia (ver "Activación automática de la licencia (explicada)" en la página 75), recuerde activar sus licencias manualmente antes de que expire el período de gracia. Si usted no tiene el archivo de licencia de software, póngase en contacto con su distribuidor XProtect.

- Tiene su **nueva versión del producto** listo. Puede descargarlo desde la página de descarga en el Milestone sitio web (http://www.milestonesys.com/downloads).
- Asegúrese de que ha respaldado la configuración del sistema (ver "Copia de seguridad y restauración de la configuración del sistema (explicado)" en la página 449).

  El servidor de gestión almacena la configuración del sistema en una base de datos. La base de datos de la configuración del sistema puede almacenarse de dos formas distintas:

  1. En una base de datos SQL Server Express Edition en el propio servidor de gestión.
  2. En una base de datos SQL Server existente en su red.

  Si utiliza 2), debe tener **derechos de administrador en SQL Server** siempre que desee crear, mover o actualizar la base de datos de configuración del sistema del servidor de administración en SQL Server. Una vez que haya terminado de crear, mover o actualización, es suficiente para ser el propietario de la base de la base de datos de configuración del sistema del servidor de gestión en el servidor SQL.

Cuando esté listo para iniciar la actualización, siga los Mejores prácticas para actualizar (en la página 60).

Mejores prácticas para actualizar

Lea sobre los requisitos de actualización (en la página 59) incluyendo la copia de seguridad de base de datos SQL antes de iniciar la actualización real.

Si su sistema es **Único equipo**, simplemente puede instalar el nuevo software encima de la instalación existente.

Nota: Los controladores de dispositivo ahora se dividen en dos paquetes de dispositivo: el paquete de dispositivo regular con controladores más nuevos y un paquete de dispositivo heredado con controladores más antiguos. El paquete de dispositivo regular siempre se instala automáticamente con una actualización. Si tiene cámaras antiguas que usan controladores de dispositivo del paquete de dispositivo heredado, **y** no tiene un paquete de dispositivo heredado ya instalado, el sistema no instala automáticamente el paquete de dispositivo heredado.

Si su sistema tiene cámaras antiguas, Milestone recomienda que compruebe si las cámaras usan controladores del paquete de dispositivo heredado en esta página (https://www.milestonesys.com/community/business-partner-tools/device-packs/). Para verificar si ya tiene instalado el paquete heredado, busque en las carpetas del sistema XProtect. Si necesita descargar el paquete de dispositivo heredado, vaya a página de descarga (http://www.milestonesys.com/downloads).

En una sistema Milestone Interconnect o Milestone Federated Architecture, debe empezar a actualizar el sitio central y después los sitios remotos.

Realizar la actualización en este orden:

1. Actualizar el servidor de gestión con la opción **Distribuida** en el instalador.
   1. En la página del asistente donde se elige componentes, todos los componentes de servidor de gestión están preseleccionados.
   2. Especificar el servidor SQL, y optar por mantener la base de datos.

Al iniciar la instalación, pierde la funcionalidad del servidor de conmutación por error.

2. Actualizar los servidores failover. Desde la página web de descarga del servidor de gestión (controlado por el Download Manager), instale el servidor de grabación.

   En este punto, la funcionalidad del servidor failover funciona de nuevo.

3. Actualizar los servidores de grabación. Puede instalar servidores de grabación utilizando el asistente de instalación (ver "Instale el servidor de grabación" en la página 44) o silenciosa (ver "Instalar un servidor de grabación en silencio" en la página 45). La ventaja de una instalación silenciosa es que se puede hacer de forma remota.

4. Actualizar el servidor de eventos. Desde la página web de descarga del servidor de gestión, instale el servidor de eventos.

Continúe estos pasos para los otros sitios en su sistema.

Actualización alternativa para el grupo de trabajo

Si no se utiliza una configuración de dominio, pero una configuración de grupo de trabajo, debe hacer lo siguiente cuando se actualiza:

1. En el servidor de grabación, cree un usuario de Windows local.

2. Desde el **panel de control** Windows, busque el **servicio Milestone XProtect Data Collector**. Haga clic con el botón derecho en él, seleccione **Propiedades** y seleccione la ficha **Inicie sesión**. Establezca el servicio Data Collector para que se ejecute como el usuario de Windows local que acaba de crear en el servidor de grabación.

3. En el servidor de gestión, crear el mismo usuario local de Windows (con el mismo nombre de usuario y contraseña).

4. En el Management Client, añadir a este usuario de Windows local para el grupo **Administrador**.

Para la instalación con los grupos de trabajo, ver Instalación para grupos de trabajo (ver "Instalación de grupos de trabajo" en la página 48).

Primer uso

Prácticas recomendadas

Proteger las bases de datos de grabación ante posible corrupción

Puede seleccionar qué acción tomar si una base de datos de la cámara se daña. Las acciones incluyen varias opciones de reparación de bases de datos. Si bien es bueno tener estas opciones, Milestone recomienda que tome medidas para asegurarse de que las bases de datos de la cámara no se corrompan.

Fallo en el disco duro: proteger sus unidades

Los discos duros son dispositivos mecánicos y son vulnerables a factores externos. Los siguientes son ejemplos de factores externos que pueden dañar las unidades de disco duro y conducir a las bases de datos corruptos de la cámara:

- Vibración (asegúrese de que el servidor del sistema de vigilancia y sus alrededores son estables)
- Fuerte calor (asegúrese de que el servidor tiene una ventilación adecuada)
- Los campos magnéticos fuertes (Evitar)
- Los cortes de energía (Asegúrese de que utiliza un sistema de alimentación ininterrumpida (UPS))
- La electricidad estática (asegúrese de que se conecte a tierra si se va a manejar una unidad de disco duro).
- Fuego, agua, etc. (evitar)

Administrador de tareas de Windows: tenga cuidado cuando finaliza procesos

Cuando se trabaja en el Administrador de tareas de Windows, tenga cuidado de no poner fin a todos los procesos que afectan al sistema de vigilancia. Si termina una aplicación o un servicio del sistema haciendo clic en **Finalizar proceso** en el Administrador de tareas de Windows, el proceso no tiene la oportunidad de guardar su estado o datos antes de que se termine. Esto puede conducir a bases de datos corruptos de la cámara.

Administrador de tareas de Windows normalmente muestra una advertencia si se intenta poner fin a un proceso. A menos que esté absolutamente seguro de que termina el proceso no va a afectar el sistema de vigilancia, haga clic en **No** cuando el mensaje de advertencia le pregunta si realmente desea terminar el proceso.

Los cortes de energía: utilizar un UPS

La razón individual más común para las bases de datos corruptos es el servidor de grabación de ser cerrado bruscamente, sin que los archivos que se guardan y sin el sistema operativo que se esté cerrado correctamente. Esto puede suceder debido a los cortes de energía, debido a que alguien accidentalmente sacando el cable de alimentación del servidor, o similar.

La mejor manera de proteger sus servidores de grabación de ser cerrado bruscamente es dotar a cada uno de sus servidores de grabación con un SAI (Sistema de Alimentación Ininterrumpida).

El SAI funciona como una fuente de energía secundaria que funciona con pilas, que proporciona la energía necesaria para guardar los archivos abiertos y segura de apagar el sistema en caso de irregularidades de

potencia. UPS varían en complejidad, pero muchos UPS incluye el software para guardar automáticamente los archivos abiertos, para alertar a los administradores de sistemas, etc.

Seleccionar el tipo de UPS para el entorno de su organización es un proceso individual. Al evaluar sus necesidades, sin embargo, tener en cuenta la cantidad de tiempo de ejecución se requiere el UPS sea capaz de proporcionar si falla el suministro. Cómo guardar los archivos abiertos y cierre de un sistema operativo correctamente puede tardar varios minutos.

Horario de verano (explicado)

El horario de verano (DST) es la práctica de avanzar los relojes para las tardes para tener más luz del día y mañanas para tener menos.El uso de horario de verano varía entre países / regiones.

Cuando se trabaja con un sistema de vigilancia, que es inherentemente sensible al tiempo, es importante que sepa cómo maneja el sistema DST.

Importante: No cambie la configuración de DST cuando esté en el período de DST o si tiene grabaciones de un período de DST.

Primavera: Cambiar desde la hora estándar al horario de verano

El cambio de la hora estándar al horario de verano no es un gran problema, ya que saltar adelanta una hora.

Ejemplo:

El reloj va hacia delante desde las 02:00 hasta las 03:00 hora estándar horario de verano, y el día tiene 23 horas. En ese caso, no hay datos 02:00-03:00 de la mañana ya que hora, para ese día, no existía.

Otoño: Cambiar de horario de verano a la hora estándar

Cuando cambia de horario de verano a la hora estándar en el otoño, saltar hacia atrás una hora.

Ejemplo:

El reloj saltos hacia atrás desde las 02:00 a 01:00 horario de verano el horario estándar, la repetición de esa hora, y el día tiene 25 horas. Llegas a 01:59:59, luego vuelves inmediatamente a 01:00:00. Si el sistema no reaccionara, básicamente volvería a registrar esa hora, por lo que la primera instancia de 01:30 sería sobrescrita por la segunda instancia de 01:30.

Para resolver una cuestión tan suceda, los archivos del sistema del vídeo actual en el caso de los cambios de tiempo del sistema por más de cinco minutos. No se puede ver la primera instancia de la hora 01:00 directamente en cualquier cliente, pero los datos se graban y segura. Puede navegar por el vídeo en XProtect Smart Client mediante la apertura de la base de datos archivados directamente.

Servidores de tiempo (explicados)

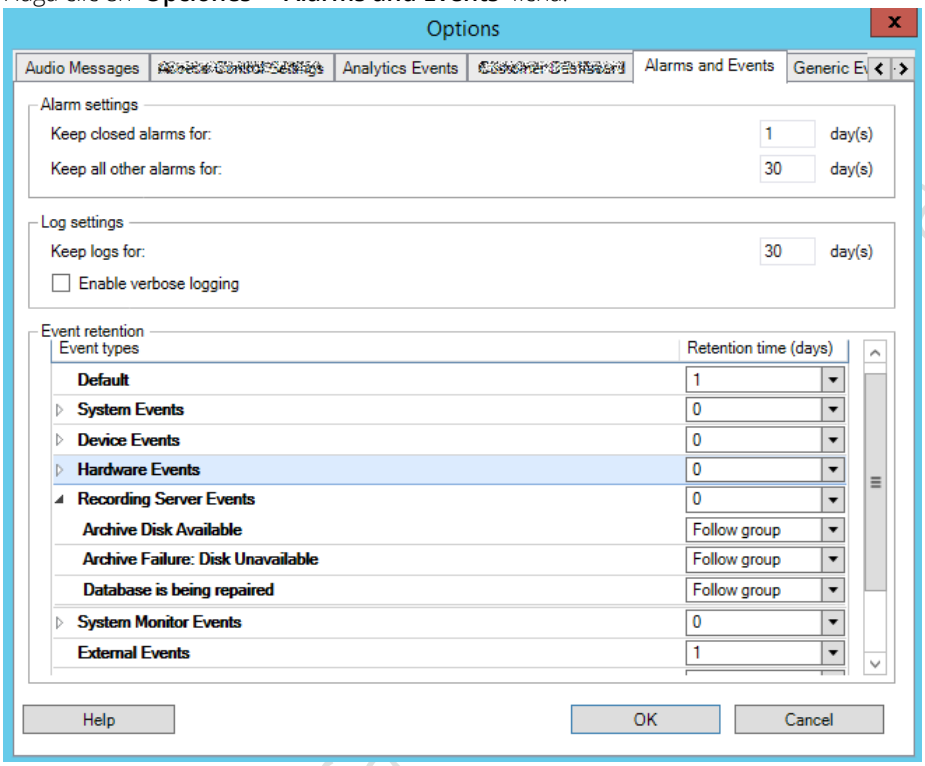
Una vez que el sistema recibe imágenes, que son al instante con marca de tiempo. Como las cámaras son unidades separadas que pueden tener dispositivos de regulación independientes, tiempo de la cámara y la hora del sistema pueden no corresponder plenamente. Esto puede en ocasiones dar lugar a confusión. Si las marcas de tiempo de apoyo a sus cámaras, Milestone recomienda que Sincronización automática de la cámara y el sistema de tiempo a través de un servidor de tiempo para la sincronización constante.

Para obtener información acerca de cómo configurar un servidor de tiempo, buscar el sitio web Microsoft (http://www.microsoft.com/) para **'servidor de tiempo'**, ' **servicio de tiempo'**, o términos similares.

Limitar el tamaño de la base de datos

Para evitar que la de base de datos (ver "SQL server" en la página 20) crezca hasta un tamaño que afecte al rendimiento del sistema, puede especificar cuántos días se almacenan en la base de datos los diferentes tipos de eventos y alarmas.

1. Abra el menú **Herramientas** .
2. Haga clic en **Opciones** > **Alarms and Events** ficha.



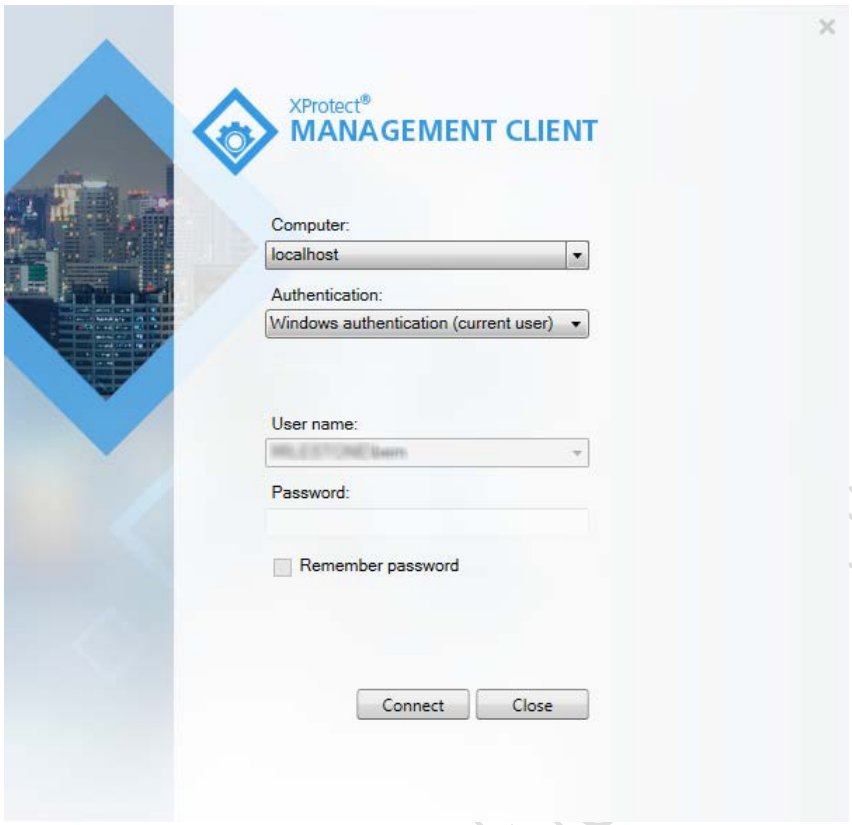
3. Realice los ajustes necesarios. Para obtener más información, consulte pestaña Alarms and Events (ver "Ficha Alarmas y eventos (opciones)" en la página 290).

Resumen de Management Client

Visión general de inicio de sesión

Cuando se inicia el Management Client, primero debe introducir su información de acceso para conectarse a un sistema.

Con XProtect Corporate 2016 o XProtect Expert 2016 o posterior instalado, puede iniciar sesión en sistemas que ejecutan versiones anteriores del producto después de instalar un parche. Las versiones compatibles son XProtect Corporate 2013 y XProtect Expert 2013 o más reciente.



Autorización de inicio de sesión (explicada)

El sistema permite a los administradores configurar los usuarios por lo que sólo pueden iniciar sesión en un sistema si un segundo usuario con derechos suficientes autorice su entrada. En este caso, XProtect Smart Client o el Management Client solicita una segunda autorización durante el inicio de sesión.

Un usuario asociado al cometido **Administradores** siempre tiene permiso para autorizar y no se le pide un segundo inicio de sesión, a menos que el usuario esté asociado con otra cometido que requiera un segundo inicio de sesión.

Para asociar la autorización de inicio de sesión con un cometido:

- Establecer **Es necesaria la autorización del inicio de sesión** para el cometido seleccionado en la ficha **Info** (ver "**Pestaña Información (cometidos)**" en la página 232) bajo **cometidos**, por lo que se le pide al usuario para la autorización adicional durante el inicio de sesión.
- Establecer **Autorizar usuarios** para el cometido seleccionado en la pestaña **Seguridad general** (ver "**Pestaña de Seguridad General (cometidos)**" en la página 234) bajo **cometidos**, de modo que el usuario puede autorizar a los inicios de sesión de otros usuarios.

Puede elegir dos opciones para el mismo usuario. Esto significa que el usuario se le pide autorización adicional durante la conexión, pero también puede autorizar a los inicios de sesión de otros usuarios, a excepción de su / su propio.

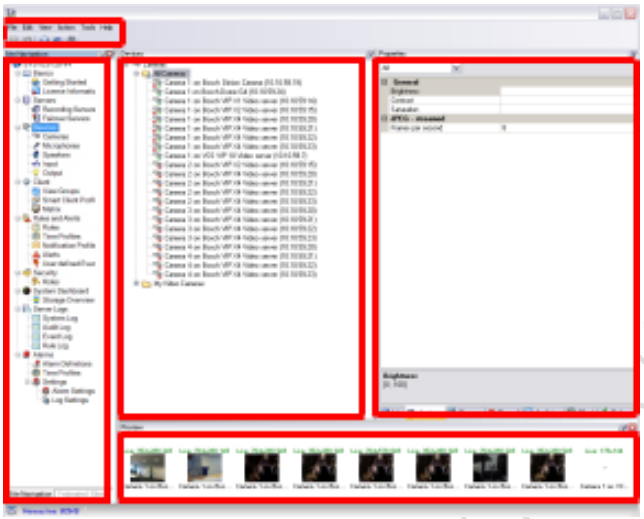
Resumen de la ventana Management Client

La ventana Management Client se divide en dos paneles. El número de paneles y distribución depende de su:

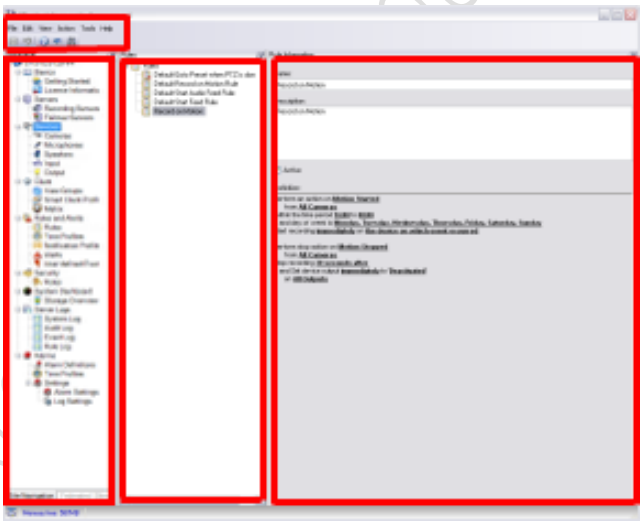
- configuración del sistema
- tarea
- funciones disponibles.

A continuación le mostramos algunos ejemplo de las distribuciones típicas:

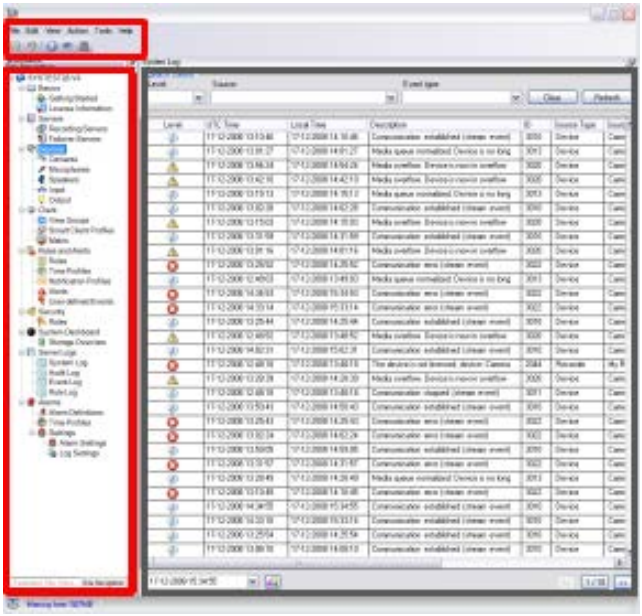
- Cuando trabaja con servidores de grabación y dispositivos:



- Cuando trabaja con reglas, perfiles horarios y notificaciones, usuarios, roles:

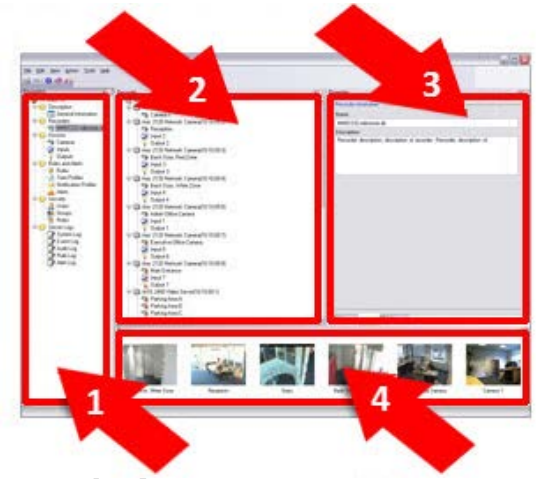


- Cuando visualiza registros:



Visión general de paneles

La ilustración describe una disposición típica ventana. Usted puede personalizar el diseño de lo que puede ser diferente en su equipo.



1. Sitio panel de navegación y el panel de la Jerarquía de sitios federados
2. Panel de generalidades
3. Panel de propiedades
4. Panel Vista previa

Panel de navegación del sitio: Este es el elemento principal de navegación del Management Client. Refleja el nombre, la configuración y las configuraciones del sitio que ha iniciado sesión en. El nombre del sitio es visible en la parte superior del panel. Las características se agrupan en categorías que reflejan la funcionalidad del software.

Panel de jerarquía de sitios federados: Este es el elemento de navegación que muestra todos los sitios Milestone Federated Architecture en una jerarquía de sitios principales/secundarios hijo.

Se puede seleccionar cualquier sitio, ingrese en él y del Management Client para que los lanzamientos del sitio. El sitio que está conectado a, es siempre en la parte superior de la jerarquía.

Panel de visión general: Proporciona una visión general del elemento que ha seleccionado en el panel **Navegación del sitio**, por ejemplo como una lista detallada. Cuando selecciona un elemento en el panel **Descripción general**, normalmente muestra las propiedades en el panel **Propiedades**. Cuando se haga clic en los elementos en el panel **general**, tendrá acceso a las funciones de administración.

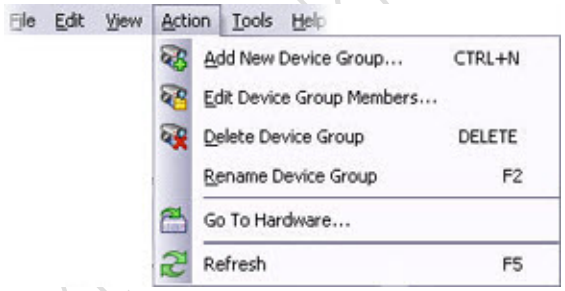
Panel Propiedades: Muestra las propiedades del elemento seleccionado en el panel **Descripción general**. Las propiedades aparecen en varias pestañas dedicadas:

Panel de vista previa: El panel **Previsualizar** aparece cuando trabaja con servidores y dispositivos de grabación. Muestra imágenes de vista previa de la muestra seleccionada cámaras o información sobre el estado del dispositivo. El ejemplo muestra una imagen de la cámara de vista previa con información acerca de la resolución y la velocidad de datos de transmisión en vivo de la cámara:

Por defecto, la información se muestra con las imágenes de la cámara de vista previa en vivo preocupaciones corrientes. Esto se muestra en el texto en verde por encima de la vista previa. Si desea grabar información de la corriente en vez (texto rojo), seleccione **Vista** > **Mostrar flujos de grabación** en el menú.

El rendimiento puede verse afectado si el panel **Previsualizar** muestra imágenes de vista previa de muchas cámaras a una velocidad de fotogramas alta. Para controlar el número de imágenes de vista previa, y su velocidad de fotogramas, seleccione **Opciones** > **general** en el menú.

Descripción del menú



Ejemplo solamente: algunos menús cambian dependiendo del contexto.

Menú Archivo

Puede guardar los cambios en la configuración y salir de la aplicación. También puede realizar una copia de seguridad de la configuración, consulte Copia de seguridad y restauración de la configuración del sistema (explicado) (en la página 449).

Editar menú

Puede deshacer cambios.

Ver menú

Nombre	Descripción
Restablecer distribución de la interfaz	Restaura la distribución de los diferentes paneles en Management Client a sus ajustes predefinidos.
Ventana de previsualización	Active o desactive el panel de **Previsualización** cuando trabaje con servidores de grabación y dispositivos.
Mostrar flujos de grabación	De manera predeterminada, la información que se muestra con las imágenes previas en el panel de **Previsualización** es relativa a los flujos en directo de las cámaras. Si quiere recibir información sobre los flujos de grabación, seleccione **Mostrar flujos de grabación**.
Jerarquía de sitios federados	De manera predeterminada, el panel de **Jerarquía federada del sitio** está activado.
Navegación del sitio	De manera predeterminada, el panel de **Navegación del sitio** está activado.

Menú Acción

El contenido del **Acción** menú difiere en función del elemento que ha seleccionado en el **Navegación del sitio** panel. Las acciones que puede elegir son las mismas que cuando hace clic con el botón derecho en el elemento. Los elementos se describen en los elementos Management Client (ver "Elementos Management Client" en la página 71).

Nombre	Descripción
Actualizar	Está siempre disponible y vuelve a cargar la información requerida del servidor de gestión.

Menú Herramientas

Nombre	Descripción
Servicios registrados	Administrar servicios registrados. Ver Canal de servicio (explicado) (en la página 471).
Servidores Professional VMS	Agregue servidores XProtect Professional VMS a su sistema y administre la integración de los servidores agregados. Ver Servidores XProtect Professional VMS (explicados) (en la página 440). También puede utilizar la función para migrar de un sistema XProtect Professional VMS a XProtect VMS. Esto se describe en un documento separado. Sólo se admite si el sistema: - Utiliza IPv4 - funciona con servidores XProtect Professional VMS que ejecutan XProtect Professional VMS versión 7.0 y superiores
Cometidos eficaces	Vea todos los cometidos de un usuario o grupo seleccionado.
Opciones	Abre la casilla de diálogo de Opciones, que le permite definir y modificar los ajustes globales del sistema.

Menú de ayuda

Puede acceder al sistema de ayuda e información sobre la versión del Management Client.

Elementos Management Client

Conceptos básicos

Información de licencia

Puede hacer un seguimiento de todas las licencias que comparten el mismo archivo de licencia de software, tanto en este sitio y en todos los demás sitios, sus suscripciones Milestone Care y decidir cómo desea activar sus licencias. Para obtener información básica acerca de las diferentes licencias XProtect, consulte Licencias (explicadas) (en la página 23).

Licenciado para

Muestra los datos de contacto del propietario de la licencia que ha introducido durante el registro del software. Haga clic en **Editar detalles** para editar la información del propietario de la licencia. Aquí también se puede encontrar un enlace al contrato de licencia de usuario final, que se aceptó antes de la instalación.

Milestone Care

Aquí se puede ver información sobre su nivel actual Milestone Care™. Cuando compró su sistema, también ingresó una suscripción Milestone Care Plus de dos años.Su instalación siempre está cubierta por Milestone Care Basic que le da acceso a diferentes tipos de material de autoayuda como artículos de base de conocimientos, guías y tutoriales en nuestro sitio web de asistencia (http://www.milestonesys.com/support). Una suscripción Milestone Care Plus le da acceso a las actualizaciones. También recibirá acceso al servicio Customer Dashboard (Panel del Cliente), la función Smart Connect y la funcionalidad completa de Notificación Push. La fecha de vencimiento de la suscripción Milestone Care Plus está visible en la **Productos instalados** tabla. Si tiene una suscripción Milestone Care Premium, también puede contactar con Milestone para recibir asistencia. Recuerde incluir información sobre su ID Milestone Care cuando contacte con la asistencia de Milestone. De nuevo, la fecha de caducidad de su suscripción Milestone Care Premium está visible. Para obtener más información sobre Milestone Care, seguir los enlaces. Si ha decidido comprar o renovar una suscripción Milestone Care después de instalar el sistema, debe activar las licencias para visualizar la información Milestone Care correcta.

Productos instalados

Lista la siguiente información acerca de todas sus licencias de base instaladas para XProtect VMS y los productos complementarios de que comparten el mismo archivo de licencia de software:

- Productos y versiones
- Código de licencia de software de los productos (SLC).
- La fecha de caducidad de su SLC. Normalmente, ilimitado.
- La fecha de vencimiento de su suscripción Milestone Care Plus.
- La fecha de vencimiento de su suscripción Milestone Care Premium.

Nota: Algunas licencias, como XProtect Essential+, no incluyen la opción para Milestone Care Plus o Milestone Care Premium, y estas columnas no aparecerán en la ventana.

Installed Products

Product Version	Software License Code	Expiration Date	Milestone Care Plus	Milestone Care Premium
XProtect Corporate 2016	M01-C01-100-01-	Unlimited	01-10-2016	01-10-2016
Milestone XProtect Smart Wall	M01-P03-023-01-	Unlimited	Unlimited	
Milestone XProtect Access 2016 v10.0a	M01-P01-011-01-	Unlimited	Unlimited	
Milestone XProtect Transact 2016	M01-P08-100-01-	Unlimited	Unlimited	

Descripción de la licencia - Todos los sitios

Enumera el número de licencias de dispositivos de hardware activadas u otras licencias en el archivo de licencia del software y el número total de licencias disponibles en su sistema.Aquí se puede ver fácilmente si todavía se puede hacer crecer su sistema sin necesidad de adquirir licencias adicionales.

Para obtener una descripción detallada del estado de sus licencias activadas en otros sitios, haga clic sobre enlace **Detalles de licencia - Todos los sitios**. Ver los **detalles de la licencia - sitio actual** a continuación para obtener la información disponible.

License Overview - All sites License Details - All Sites...

License Type	Activated
Hardware Device	51 out of 100
Milestone Interconnect Camera	0 out of 100
Access control door	9 out of 2002
Transaction source	1 out of 101

Si tiene licencias para productos add-on, se puede ver detalles adicionales sobre estos en los nodos específicos de productos add-on en el **Panel de Navegación del sitio**.

Detalles de la licencia - Sitio Actual

La columna **Activado** incluye el número de licencias de dispositivos de hardware activados u otras licencias en este sitio.

También puede ver el número de cambios de dispositivo utilizado sin activación (ver "Cambios de dispositivo sin activación (explicado)" en la página 73) y el número que tiene disponible por año en la columna **modificaciones efectuadas sin activación**.

Si tiene licencias que aún no se han activado y que, por lo tanto, se ejecutan en un período de gracia, se enumeran en la columna **En período de gracia**. La fecha de vencimiento de la primera licencia que expira, aparece en rojo debajo de la mesa.

Si se olvida de activar las licencias antes de que expire el período de gracia, van a dejar de enviar vídeo al sistema. Estas licencias se muestran en la columna **Período de gracia expirado**. Véase también licencias se activa después de período de gracia (ver "Activar las licencias después de período de gracia" en la página 76).

Si ha utilizado más licencias que las que tiene disponibles, estas se enumeran en la columna **Sin licencia** y no se pueden utilizar en su sistema. Ver también Obtener licencias adicionales (en la página 77).

Si tiene licencias en un período de gracia, con un período de gracia ha expirado o sin licencia, un mensaje aparecerá para recordarle cada vez que se acceda a su Management Client.

License Details - Current Site: SYS

License Type	Activated	Changes without activation	In Grace Period	Grace Period Expired	Without License
Hardware Device	32	0 out of 10	0	0	0
Milestone Interconnect Camera	11	N/A	0	0	0
Access control door	9	N/A	0	0	0
Transaction source	1	N/A	0	0	0

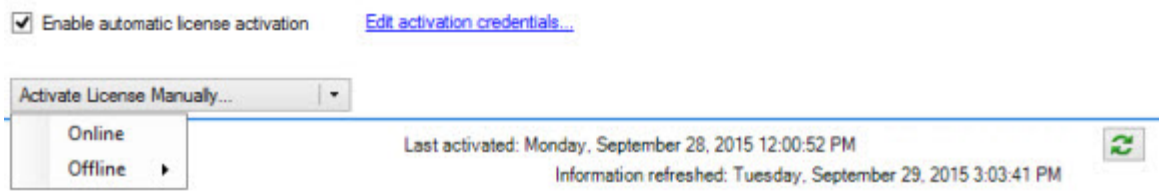
Los dispositivos de hardware sin licencia son identificados por un signo de exclamación en el Management Client. Tenga en cuenta que el signo de exclamación también se utiliza para otros fines. Coloca el ratón sobre el signo de exclamación al ver el fin.

Características para la activación de licencias

Por debajo de las tres mesas están

- Una casilla de verificación para permitir la activación automática de la licencia y un enlace para editar las credenciales de usuario para la activación automática. Para obtener más información, consulte Activación automática de la licencia (explicada) (en la página 75) y Activar la activación automática de la licencia (en la página 75). Si la activación automática no ha funcionado, un mensaje no aparecerá en rojo. Para obtener más información, haga clic en el enlace **Detalles**.
- Una lista desplegable para activar manualmente los certificados en línea o fuera de línea. Para obtener más información, consulte Activar licencias en línea (en la página 76) y Activar licencias sin conexión (ver "Activar las licencias en línea" en la página 76).
- En la esquina inferior derecha de la página, se puede ver cuando las licencias se activaron pasado (automática o manualmente) y cuando las informaciónes de la página fueron actualizadas. Las marcas de tiempo son desde el servidor y no desde el equipo local.

Nota: Algunas licencias, como XProtect Essential+, se instalan con la activación automática de licencias activada y no es posible desactivar esta configuración.



Cambios de dispositivo sin activación (explicado)

En la página **Básico** > **Información de licencia**, la columna **Cambios sin activación** muestra el número de dispositivos de hardware que puede reemplazar o añadir sin tener que activar las licencias de sus dispositivos de hardware y cuántos cambios ya ha realizado desde la última activación. Los dispositivos de hardware agregados dentro de su dispositivo cambian sin que la activación se ejecute como licencias de dispositivo de hardware completamente activadas. Un año después de su última activación de licencia, su número de **modificaciones de dispositivo sin activación** se restablece automáticamente a cero. Una vez que el reinicio ocurre, puede seguir añadir y reemplazar los dispositivos de hardware sin necesidad de activar las licencias.

El número de cambios de dispositivo sin activación difiere de una instalación a otra, y se calcula en función de diversas variables. Para una descripción detallada, ver ¿Cómo se calcula el número de cambios de dispositivo sin activación (en la página 74).

Si su sistema de vigilancia está fuera de línea durante períodos más largos de tiempo, por ejemplo, en los casos con un sistema de vigilancia en un barco en un largo crucero o un sistema de vigilancia en un lugar muy remoto sin ningún tipo de acceso a Internet, puede ponerse en contacto con el distribuidor Milestone y solicitar un mayor número de cambios de dispositivo sin activación.

Usted debe explicar por qué cree que usted tiene derecho a un mayor número de cambios de dispositivo sin activación. Milestone decide cada solicitud de forma individual. En caso de que le otorgará un mayor número de cambios de dispositivo sin activación, debe activar las licencias para registrar el número más alto en su sistema XProtect.

¿Cómo se calcula el número de cambios de dispositivo sin activación

Los cambios de dispositivo sin activación se calculan en función de tres variables. Si tiene varias instalaciones del software de Milestone, las variables se aplican a cada uno de ellos por separado. Las variables son:

- **C%** que es un porcentaje fijo de la cantidad total de licencias activadas.
- **Cmin** que es un valor mínimo fijo del número de cambios de dispositivo sin activación.
- **Cmax** que es un valor máximo fijo de la cantidad de dispositivos cambios sin activación.

El número de cambios de dispositivo sin activación nunca puede ser inferior al valor **Cmin** o superior al valor **Cmax**. El valor calculado basado en la variable **C%** cambia según el número de dispositivos activados que tiene en cada instalación de su sistema. Los dispositivos agregados con los cambios de dispositivos sin activación no se cuentan como activado por el **C%** variable.

Milestone define los valores de las tres variables y los valores están sujetos a cambios sin notificación. Los valores de las variables varían en función del producto.

Para obtener más información sobre los valores predeterminados actuales de su producto, vaya a My Milestone (http://www.milestonesys.com/device-change-calculation).

Ejemplos basados en C% = 15%, Cmin y Cmax = 10 = 100

Un cliente compra 100 licencias de dispositivos de hardware. Y añade 100 cámaras a su sistema. A menos que él ha permitido la activación automática de la licencia, sus cambios de dispositivo sin activación siguen siendo cero. Se activa sus licencias y ahora tiene 15 cambios de dispositivo sin activación.

Un cliente compra 100 licencias de dispositivos de hardware. Y añade 100 cámaras a su sistema y activa sus licencias. Sus cambios de dispositivo sin activación es ahora 15. El cliente decide eliminar un dispositivo de hardware de su sistema. Ahora tiene 99 dispositivos activados y su número de cambios de dispositivo sin activación se reduce a 14.

Un cliente compra 1000 licencias de dispositivos de hardware. Y añade 1000 cámaras y activa sus licencias. Sus cambios de dispositivo sin activación es ahora 100. De acuerdo con la **C%** variables, que ahora debería haber tenido 150 dispositivos cambios sin activación, pero el variable de **Cmax** sólo se le permite tener 100 dispositivos cambios sin activación.

Un cliente compra 10 licencias de dispositivos de hardware. Y añade 10 cámaras a su sistema y activa sus licencias. Su número de cambios de dispositivo sin activación es ahora 10 debido a la variable **Cmin**. Si el número solamente se calculó en base a la **C%** variables, que sólo habría tenido 1 (15% de 10 = 1,5 redondeado a 1).

Un cliente compra 115 licencias de dispositivos de hardware. Y añade 100 cámaras a su sistema y activa sus licencias. Sus cambios de dispositivo sin activación es ahora 15. Se añade otros 15 cámaras sin activarlos, utilizando 15 de los 15 de sus cambios de dispositivo sin activación. Se elimina 50 de las cámaras del sistema y sus cambios de dispositivo sin activación baja a 7. Esto significa que 8 de las cámaras añadido previamente dentro de los 15 cambios de dispositivo sin activación entrar en un período de gracia. Ahora el cliente añade 50 nuevas cámaras. Debido a que el cliente activa 100 cámaras en su sistema la última vez que activó sus licencias, los cambios de dispositivo sin activación se remontan a 15 y las 8 cámaras, las cuales fueron trasladadas a un período de gracia, se mueve hacia atrás como los cambios de dispositivos sin activación. Las 50 nuevas cámaras entran en un período de gracia.

Ver visión general licencia

Puede acceder a una visión general de licencia que las listas de licencias que se activan, en un período de gracia, expirado y faltante para todos los sitios con licencia a través del mismo archivo de licencia de software.

- Haga clic en **Descripción de la licencia**.

Si el sitio no es un sitio federada o la conexión es baja, sólo se puede ver el número de licencias activadas. N / A aparece por licencias en un período de gracia, licencias caducadas y licencias que faltan.

Activación automática de la licencia (explicada)

Para facilitar el mantenimiento y la flexibilidad, Milestone recomienda que habilite la activación automática de la licencia (ver "Activar la activación automática de la licencia" en la página 75) porque significa menos mantenimiento para usted. La activación automática de licencias requiere que su servidor de gestión esté en línea.

Cuando se cumplen los requisitos anteriores, el sistema activa sus dispositivos de hardware u otras licencias unos minutos después de agregar, eliminar o reemplazar dispositivos de hardware o realizar otros cambios que afectan al uso de sus licencias. Por lo tanto, nunca se tiene que iniciar manualmente una activación de la licencia, el número de cambios de dispositivo usadas sin activación es siempre cero y no hay dispositivos de hardware se encuentran dentro de un período de gracia y están en riesgo de expirar. Si uno de sus licencias de base vencen en un plazo de 14 días, su sistema XProtect también - como precaución extra - prueba automática para activar sus licencias cada noche.

La única vez que usted tiene que activar manualmente las licencias, es cuando se ha comprar licencias adicionales (ver "Obtener licencias adicionales" en la página 77), quieren actualización (ver "Requisitos de actualización" en la página 59), si ha comprado o renovado un Milestone Care suscripción (ver "Información de licencia" en la página 71), o si Milestone le ha otorgado un mayor número de cambios de dispositivo sin activación (ver "Cambios de dispositivo sin activación (explicado)" en la página 73).

Activar la activación automática de la licencia

1. En la página **Información de licencia**, seleccione **Permitir la activación automática de la licencia**.
2. Introduzca el nombre de usuario y la contraseña que desea utilizar con la activación automática de la licencia. Las credenciales se guardan en un archivo en el servidor de gestión.
   - Si usted es un usuario existente, introduzca su nombre de usuario y contraseña para iniciar sesión en el sistema de registro de software.
   - Si es un usuario nuevo, haga clic en el enlace **Crear nuevo usuario** para configurar una nueva cuenta de usuario y luego siga el procedimiento de registro. Si aún no ha registrado su código de licencia de software (SLC), debe hacerlo.
3. **Haga clic en OK (aceptar)**.

Si más adelante desea cambiar su nombre de usuario y / o la contraseña de activación automática, haga clic en enlace **modificar las credenciales activación**.

Deshabilitar la activación automática de la licencia

Deshabilitar la activación automática de la licencia, pero mantener la contraseña para su uso posterior

- En la página **Información de licencia**, deseleccione **Permitir la activación automática de la licencia**. La contraseña y nombre de usuario todavía se guardan en el servidor de gestión.

Deshabilitar la activación automática de la licencia y eliminar la contraseña

- En la página **Información de licencia**, haga clic en **Editar credenciales de activación**.
- Haga clic en **Eliminar contraseña**.
- Confirme que desea eliminar la contraseña y nombre de usuario del servidor de gestión.

Activar licencias en línea

Activar sus licencias en línea si el equipo que ejecuta el servidor de gestión tiene acceso a Internet.

1. En el nodo de **Información de licencia**, seleccione **Activar licencia manualmente** y luego **Línea**.
2. Se abre el cuadro de diálogo **Activar en línea**.
   - Si usted es un usuario existente, introduzca su nombre de usuario y contraseña.
   - Si es un usuario nuevo, haga clic en el enlace **Crear nuevo usuario** para configurar una nueva cuenta de usuario. Si aún no ha registrado su código de licencia de software (SLC), debe hacerlo.
3. **Haga clic en OK (aceptar)**.

Si recibe un mensaje de error durante la activación en línea, siga las instrucciones de la pantalla para resolver el problema. Si ha seguido las instrucciones y todavía no puede acceder a la activación en línea (https://www.milestonesys.com/OnlineActivation/LicenseManagementService.asmx), póngase en contacto con Milestone Support.

Activar las licencias en línea

Si el equipo que ejecuta el servidor de gestión no tiene acceso a Internet, puede activar las licencias en línea.

1. En el nodo de **información de licencia**, seleccione **Activar licencia manualmente** -> **Desconectado** -> **Exportar licencia para su activación** para exportar un archivo de solicitud de licencia (. lrq) con información acerca de los dispositivos de hardware añadidos.
2. El archivo de solicitud de licencia (. lrq) recibe automáticamente el mismo nombre que el SLC. Si tiene varios sitios, recuerde que debe hacer el nombre único por lo que fácilmente puede identificar qué archivo pertenecen a qué sitio.
3. Copiar el archivo de solicitud de licencia para una computadora con acceso a Internet y acceder a nuestra página web (http://online.milestonesys.com) para obtener el archivo de licencia de software activado (.lic).
4. Copiar el archivo .lic que tiene el mismo nombre que el archivo de solicitud de licencia para el equipo con Management Client.
5. En Management Client en la página de **información de licencia**, seleccione **Activar licencia fuera de línea** > **Importar licencia activada** y seleccione el archivo de licencia de software activado para importarlo y con ello activar sus licencias.
6. Haga clic en **Finalizar** para finalizar el proceso de activación.

Activar las licencias después de período de gracia

Si no activa una licencia (dispositivo de hardware, la cámara de Milestone Interconnect, o las licencias de puertas de control de acceso) dentro del período de gracia, el dispositivo deja de estar disponible y no puede enviar los datos al sistema de vigilancia.

- El dispositivo en sí, su configuración y otros ajustes no se eliminan de la configuración del sistema.
- Para ser capaz de recibir datos desde el dispositivo expirado nuevo, basta con activar la licencia. Para obtener más información, consulte Activar las licencias fuera de línea (ver "Activar las licencias en línea" en la página 76) o Activar las licencias en línea (ver "Activar licencias en línea" en la página 76).

Obtener licencias adicionales

Si desea añadir o si ya ha añadido más dispositivos de hardware, sistemas de Milestone Interconnect, o puertas de lo que actualmente tienen licencias para, usted debe comprar licencias adicionales para permitir que los dispositivos para enviar datos a su sistema.

- Para obtener licencias adicionales para su sistema, póngase en contacto con su distribuidor de productos XProtect.

Las nuevas licencias a la versión del sistema de vigilancia existente:

- Basta con activar las licencias de forma manual para obtener acceso a las nuevas licencias. Para obtener más información, consulte Activar las licencias fuera de línea (ver "Activar las licencias en línea" en la página 76) o Activar las licencias en línea (ver "Activar licencias en línea" en la página 76).

Éstos y una versión mejorada del sistema de vigilancia:

- Recibe un archivo de licencia de software actualizado (.**lic**) (ver "Licencias (explicadas)" en la página 23) con las nuevas licencias y la nueva versión. Debe utilizar el nuevo archivo de licencia de software durante la instalación de la nueva versión. Para obtener más información, consulte Requisitos de actualización (en la página 59).

Licencias y sustitución de dispositivos de hardware

Puede sustituir un dispositivo de hardware, tales como una cámara, con licencia en su sistema con un nuevo dispositivo de hardware, y tener el nuevo dispositivo de hardware activada y con licencia en su lugar.

Si se quita un dispositivo de hardware de un servidor de grabación, a liberar una licencia de dispositivo de hardware.

Si reemplaza una cámara con una cámara similar (fabricante, la marca y modelo), y dar a la nueva cámara de la misma dirección IP, a mantener el pleno acceso a todas las bases de la cámara. En este caso, se mueve el cable de red de la cámara vieja a la nueva sin cambiar la configuración del Management Client.

Si se reemplaza un dispositivo de hardware con un modelo diferente, se debe utilizar el asistente **Reemplazar el hardware** (ver Reemplazar el hardware (en la página 458)) para mapear todas las bases de datos pertinentes de cámaras, micrófonos, entradas, salidas, y los ajustes.

Si tiene habilitado activación automática de licencia (ver "Activar la activación automática de la licencia" en la página 75), el nuevo dispositivo de hardware se activa automáticamente. Si ha utilizado todos sus cambios de dispositivos sin activación (ver "Cambios de dispositivo sin activación (explicado)" en la página 73), debe activar manualmente sus licencias. Para obtener más información, consulte Activar las licencias fuera de línea (ver "Activar las licencias en línea" en la página 76) o Activar las licencias en línea (ver "Activar licencias en línea" en la página 76).

Información del emplazamiento

Se puede añadir información adicional a un sitio para una más fácil identificación de cada sitio, por ejemplo, en un gran Milestone Federated Architecture configuración. Aparte del nombre del sitio, se puede describir:

- Dirección / ubicación
- Administrador(es)
- Información Adicional

Actualizar la información de sitio

Para actualizar la información del sitio:

1. Seleccione **Editar**.
2. Seleccione una etiqueta.
3. Introduzca la información en el campo **Valor**.
4. **Haga clic en OK (aceptar)**.

Servidores y hardware

Servidores de grabación

Servidores de grabación (explicados)

Se utiliza servidores de grabación para la grabación de señales de vídeo, y para la comunicación con las cámaras y otros dispositivos. Un sistema de vigilancia consiste típicamente en varios servidores de grabación.

Servidores de grabación son los equipos en los que ha instalado el software de servidor de grabación, y configurados para comunicarse con un servidor de gestión. Puede ver sus servidores de grabación en el panel **Información general** cuando se expande la carpeta **Servidores** y, a continuación, seleccione **Servidores de grabación**.

La compatibilidad con las versiones de servidor de grabación anteriores de esta versión del servidor de gestión es limitada. Todavía se puede acceder a las grabaciones en los servidores de grabación con las versiones anteriores, pero si desea cambiar su configuración, asegúrese de que coincida con esta versión del servidor de gestión. Milestone recomienda que actualice todos los servidores de grabación en el sistema a la misma versión que el servidor de gestión.

Tiene varias opciones relacionadas con la gestión de los servidores de grabación:

- Autorizar un servidor de grabación (en la página 79)
- Añadir hardware (en la página 109)
- Mover hardware (en la página 112)
- Eliminar todo el hardware (ver "Eliminar todo el hardware en un servidor de grabación" en la página 100)
- Retirar un servidor de grabación (en la página 100)

Importante: Cuando el servicio Recording Server está en marcha, es muy importante que el Explorador de Windows u otros programas no tienen acceso a los archivos de base de datos multimedia o carpetas asociados a la configuración de su sistema. Si lo hacen, es probable que el servidor de grabación no puede cambiar el nombre o mover los archivos multimedia pertinentes. Esto podría llevar el servidor de grabación a un alto. Para reiniciar un servidor de grabación detenido, detener el servicio Recording Server, cierre el programa de acceso al archivo correspondiente medio (s) o carpeta (s), y reinicie el servicio de grabación de servidor.

Autorizar un servidor de grabación

Si la conexión entre su servidor de administración y su servidor de grabación está rota, debe autorizar al servidor de grabación a restablecer la conexión.

Nota: Al instalar un servidor de grabación, se autoriza automáticamente. Sólo debe autorizar un servidor de grabación si el servidor de grabación se ha eliminado del servidor de gestión y se ha vuelto a añadir.

Cuando autoriza un servidor de grabación, se configura para conectarse al servidor de gestión.

1. Haga clic con el servidor de registro que se requieren en el panel **general**.
2. Seleccionar **Autorizar Recording Server**:

3. Después de un momento, el servidor de grabación está autorizada y listo para una configuración adicional a través de las pestañas. También puede Añadir hardware (en la página 109).

Cambiar / verificar la configuración básica de un servidor de grabación

Si su Management Client no se enumeran todos los servidores de grabación que haya instalado, la razón más probable es que haya configurado los parámetros de configuración (por ejemplo, la dirección IP o nombre de host del servidor de gestión) de forma incorrecta durante la instalación.

No es necesario volver a instalar servidores de grabación para especificar los parámetros de los servidores de gestión, pero se puede cambiar / verificar su configuración básica:

1. En el equipo que ejecuta el servidor de grabación, haga clic en el icono de **Servidor de grabación** en el área de notificación.
2. Seleccionar **Detener servicio Recording Server**.
3. Haga clic en el icono del **servidor de grabación** nuevo y seleccione **cambiar la configuración**.

   Aparecerá la ventana **Recording Server Settings** (ajustes de Recording Server).
4. Verificar / modificar la configuración siguiente:

- **Nombre de host del servidor de administración / dirección IP**: Especifique la dirección IP o el nombre de host del servidor de gestión a la que el servidor de grabación debe estar conectado.
- **Puerto del servidor de administración**: Especificar el número de puerto que se utilizará cuando se comunica con el servidor de gestión. Puerto predeterminado es 9993. Puede cambiar si es necesario, pero el número de puerto siempre debe coincidir con el número de puerto configurado en el servidor de gestión.

5. **Haga clic en OK (aceptar)**.
6. Para iniciar el servicio de grabación Server de nuevo, haga clic en el icono de **servidor de grabación** y seleccione **Reiniciar servicio Recording Server**.

Importante: Detener el servicio Recording Server significa que no se puede grabar y visualizar vídeo en vivo mientras verificar / modificar la configuración básica del servidor de grabación.

Grabación de los iconos de estado del servidor

Management Client usa los siguientes iconos para indicar el estado de los servidores de grabación individuales:

Icono	Descripción
	**El servidor de grabación está en funcionamiento**
	**El servidor de grabación requiere la atención:** O el servidor de grabación no se está ejecutando o está ejecutándose con errores. 1) Desplácese sobre el icono del servidor de grabación para ver el mensaje de estado. 2) Si necesita iniciar o detener el servidor de grabación, haga clic con el botón derecho en el icono de la bandeja del Administrador del servidor de grabación (Recording Server Manager).
	**El servidor de grabación debe estar autorizado:** Aparece cuando se carga el servidor de grabación por primera vez. La primera vez que utiliza un servidor de grabación, debe autorizarlo: 1) Haga clic en el icono del servidor de grabación deseada. 2) Seleccione **Autorice el servidor de grabación**. Después de un momento, el servidor de grabación está autorizada y listo para otra configuración.
	**Reparación de bases de datos en curso:** Aparece cuando se dañan las bases de datos, por ejemplo, debido a una falla de energía, y el servidor de grabación de ellas está reparando. El proceso de reparación puede llevar algún tiempo si las bases de datos son grandes. Ver Proteger bases de datos de registro de la corrupción (ver "Proteger las bases de datos de grabación ante posible corrupción" en la página 62) para obtener información sobre cómo evitar las bases de datos corruptos. **Importante:** Durante una reparación de la base de datos en el arranque, no se puede grabar vídeo desde cámaras conectadas al servidor de grabación. Sólo visualización en directo está disponible. Una reparación de bases de datos en el funcionamiento normal no afecta a las grabaciones.

Pestaña de información (servidor de impresión)

Puede verificar o editar el nombre y la descripción de un servidor de grabación seleccionado en la pestaña **Info**.

Propiedades Pestaña Info

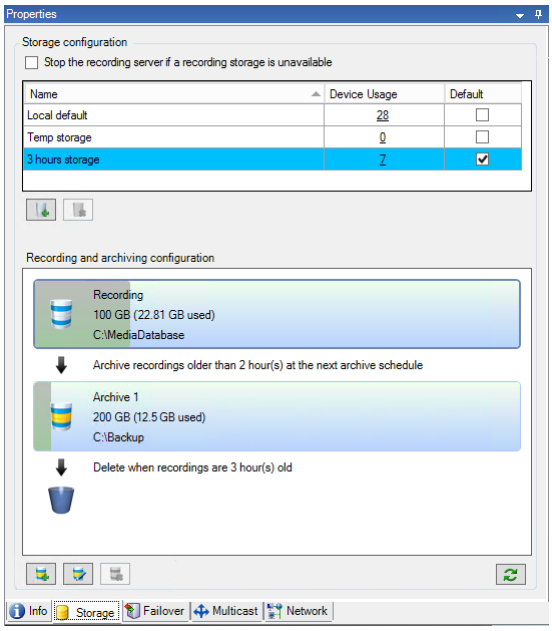
Nombre	Descripción
Nombre	Se utiliza cuando el servidor de grabación aparece en el sistema y clientes. El nombre no tiene que ser único. Al cambiar el nombre de un servidor de grabación, el nombre se cambia a nivel mundial en el Management Client.
Descripción	La descripción aparece en un número de máquinas en el sistema. Una descripción no es obligatoria.
Nombre de host	Muestra el nombre de host del servidor de grabación.
URL del servidor Web	Muestra la dirección URL del servidor web del servidor de grabación. Se utiliza el servidor web, por ejemplo, para el manejo de órdenes de control de cámara PTZ, y para el manejo de solicitudes de exploración y en directo de XProtect Smart Client. La dirección URL incluye el número de puerto utilizado para la comunicación servidor web (normalmente el puerto 7563).
Zona horaria	Muestra la zona horaria en la que se encuentra el servidor de grabación.

Pestaña de almacenamiento (servidor de grabación)

En la ficha **Almacenamiento** , puede configurar, administrar y ver los almacenes para un servidor de grabación seleccionado.

Para registrar almacenes y archivos, la barra horizontal muestra la cantidad actual de espacio libre. Puede especificar el comportamiento del servidor de grabación en caso de que los almacenamientos de grabación no estén disponibles. Esto es principalmente relevante si su sistema incluye servidores failover.

Si está utilizando **Bloqueo de evidencia**, habrá una línea roja vertical que muestra el espacio utilizado para las secuencias de pruebas de bloqueo.



Almacenamiento y archivo (explicado)

Funcionalidad disponible depende del sistema que está utilizando. Ver tabla de comparación de productos (en la página 24) para más información.

Cuando una cámara graba vídeo o audio, todas las grabaciones son especificados por defecto almacenada en el almacenamiento definida para el dispositivo. Cada almacenamiento consiste en un almacenamiento de grabación que guarda grabaciones en la base de datos de grabación **Grabando**. Un almacenamiento tiene ningún archivo (s) de forma predeterminada, pero se pueden crear estos.

Para evitar que la base de datos de grabación se ejecute completa, puede crear almacenes adicionales (ver "Añadir un nuevo almacenamiento de grabaciones" en la página 85). También puede crear archivos (ver "Crear un archivo dentro de un almacenamiento" en la página 85)dentro de cada almacenamiento y comenzar un proceso de archivo para almacenar datos.

El archivo es la transferencia automática de las grabaciones de, por ejemplo, la base de datos de grabación de una cámara a otra ubicación. De esta manera, la cantidad de grabaciones que se pueden almacenar no se limita al tamaño de la base de datos de grabación. Con el archivado también puede realizar copias de seguridad de sus grabaciones en otro medio.

Configura el almacenamiento y el archivo en cada servidor de grabación.

Siempre que almacene grabaciones archivadas localmente o en unidades de red accesibles, puede usar XProtect Smart Client para verlas.

Si una unidad de disco se rompe y el almacenamiento de la grabación deja de estar disponible, la barra horizontal se vuelve roja. Todavía es posible ver video en vivo en XProtect Smart Client, pero la grabación y el archivo se detienen hasta que se restaura la unidad de disco. Si su sistema está configurado con servidores de grabación failover, puede especificar que el servidor de grabación deje de ejecutarse, para permitir que los servidores failover se hagan cargo (ver "Especifique el comportamiento cuando la grabación del almacenamiento no está disponible" en la página 85).

La siguiente mayormente menciones cámaras y video, pero los altavoces, micrófonos, audio y sonido también se aplican.

Importante: Milestone recomienda utilizar una unidad de disco duro dedicada para registrar almacenamientos y archivos para evitar el bajo rendimiento del disco. Al formatear el disco duro, es importante cambiar su configuración **Tamaño de unidad de asignación** de 4 a 64 kilobytes. Esto es para mejorar significativamente el rendimiento de grabación del disco duro. Puede leer más acerca de la asignación de los tamaños de unidad y encontrar ayuda en el sitio web de Microsoft (http://support.microsoft.com/kb/140365/en-us).

Importante: Los datos más antiguos en una base de datos siempre han archivado automáticamente (o eliminado si no se define ningún archivo siguiente) cuando menos de 5 GB de espacio está libre. Si es menos de 1 GB de espacio es libre, se eliminan los datos. Una base de datos siempre requiere de 250 MB de espacio libre. Si se alcanza este límite ya que los datos no se eliminan lo suficientemente rápido, no hay más datos se escriben en la base de datos hasta que se libere el espacio suficiente. El tamaño máximo real de la base de datos se convierte en la cantidad de gigabytes que especifique, menos de 5 GB.

La conexión de dispositivos a un almacenamiento

Una vez que haya configurado los ajustes de almacenamiento y archivo de un servidor de grabación, puede activar el almacenamiento y archivo para cámaras individuales o un grupo de cámaras. Usted hace esto desde los dispositivos individuales o desde el grupo de dispositivos. Consulte Adjuntar un dispositivo o grupo de dispositivos a un almacenamiento (ver "Conectar un dispositivo o grupo de dispositivos a un almacenamiento" en la página 86).

Archivado eficaz

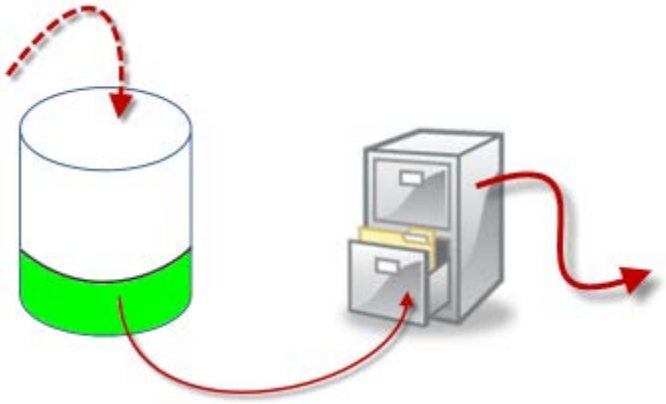
Cuando habilita el archivado para una cámara o un grupo de cámaras, el contenido del almacenamiento de grabaciónse mueve automáticamente al primer archivo en los intervalos que define usted.

Dependiendo de sus requisitos, puede configurar uno o más archivos para cada uno de sus almacenamientos. Los archivos pueden estar situados en el equipo servidor de grabación en sí, o en otro lugar que puede ser alcanzado por el sistema, por ejemplo, en una unidad de red.

Al configurar su archivo de manera efectiva, puede optimizar las necesidades de almacenamiento. A menudo, usted quiere hacer grabaciones archivadas ocupen el menor espacio posible, especialmente sobre una base a largo plazo, en el que es quizás aún posible aflojar la calidad de imagen un poco. Usted maneja el archivo efectivo de la pestaña **Almacenamiento** de un servidor de grabación ajustando varias configuraciones interdependientes:

- Retención de almacenamiento de grabación
- Tamaño de almacenamiento de grabación
- Retención de archivos
- Tamaño de archivo
- Programación de archivar
- Cifrado
- Fotogramas por segundo (FPS).

Los campos de tamaño definen el tamaño del almacenamiento de la grabación, ejemplificado por el cilindro y sus archivos, respectivamente:



Mediante el ajuste del periodo de retención y el tamaño para el almacenamiento de la grabación, ejemplificado por el área blanca del cilindro, usted define la antigüedad de las grabaciones antes de que se archiven. En nuestro ejemplo ilustrado, archivar las grabaciones cuando tengan la edad suficiente para ser archivados.

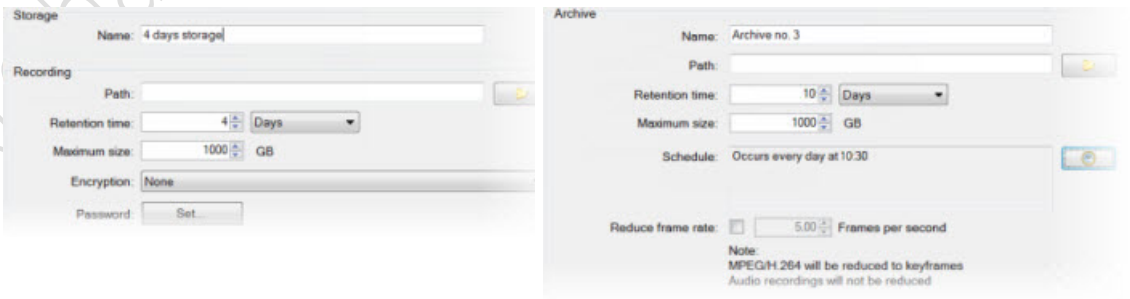
El tiempo de retención y ajuste de tamaño para los archivos definen cuánto tiempo se mantienen las grabaciones en el archivo. Las grabaciones se mantienen en el archivo durante el tiempo especificado, o hasta que el archivo ha alcanzado el límite de tamaño especificado. Cuando se cumplen estos ajustes, el sistema comienza a sobrescribir grabaciones antiguas en el archivo.

El horario de archivado define con qué frecuencia y en qué momento se lleva a cabo el archivado.

FPS determina el tamaño de los datos en las bases de datos.

Para archivar las grabaciones, es necesario configurar todos estos parámetros de acuerdo unos con otros. Esto significa que el período de retención del próximo archivo siempre debe ser más largo que el período de retención de un archivo actual o una base de datos de grabación. Esto es porque el número de días de retención declarada de un archivo incluye todos retención se dijo anteriormente en el proceso. También archivado siempre debe llevarse a cabo con mayor frecuencia que el período de retención, de lo contrario se corre el riesgo de perder datos. Si usted tiene un tiempo de retención de 24 horas, se elimina todos los datos de más de 24 horas. Por lo tanto, para obtener sus datos de forma segura trasladaron al siguiente archivo, es importante ejecutar el archivo con más frecuencia que cada 24 horas.

> **Ejemplo**: Estos almacenamientos (imagen a la izquierda) tienen un tiempo de retención de 4 días y el archivo siguiente (imagen de la derecha) un tiempo de retención de 10 días. Archivado se establece que ocurra todos los días a las 10:30, asegurando un archivo mucho más frecuente que el tiempo de retención.

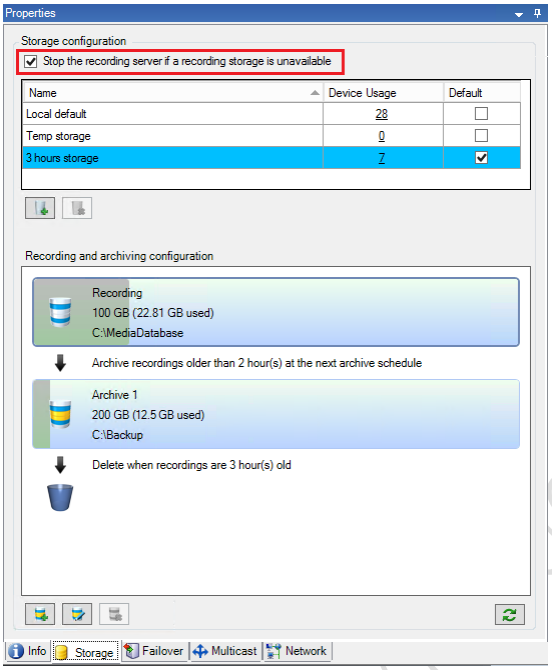


También puede controlar el archivo mediante el uso de reglas y eventos.

Especifique el comportamiento cuando la grabación del almacenamiento no está disponible

De forma predeterminada, el servidor de grabación sigue funcionando si un almacenamiento de grabación no está disponible. Si su sistema está configurado con servidores de grabación failover, puede especificar que el servidor de grabación deje de ejecutarse, para que los servidores failover se hagan cargo:

1. En el servidor de grabación relevante, vaya a la pestaña **Almacenamiento**.
2. Seleccione opción **Detener el servidor de grabación si no hay disponible un almacenamiento de grabación**.



Añadir un nuevo almacenamiento de grabaciones

Siempre crea un almacenamiento con una base de datos de grabación predefinida llamada **Grabación**. No se puede cambiar el nombre de la misma. Aparte de una base de datos de grabación, un dispositivo de almacenamiento puede contener un número de archivos.

1. Para añadir un almacenamiento adicional a un servidor de grabación seleccionado, haga clic en  botón situado debajo de la **Configuración de almacenamiento** lista. Esto abre el **Configuración de almacenamiento y grabación** caja de diálogo.
2. Especificar los ajustes (ver "Propiedades de almacenamiento y configuraciones para la grabación" en la página 91) pertinentes.
3. **Haga clic en OK (aceptar)**.

Si es necesario, que ahora está listo para crear archivo (s) dentro de su nuevo almacenamiento. Consulte Crear un archivo dentro de un almacenamiento (en la página 85).

Crear un archivo dentro de un almacenamiento

Un almacenamiento no tiene un archivo predeterminado, pero puede crear archivos según sea necesario.

1. Seleccione el almacenamiento relevante en lista **Configuración de grabación y archivado**.

2. Haga clic en el  el botón debajo de la **Configuración de grabación y archivado** lista.
3. En el cuadro de diálogo **Configuración de archivo**, especifique los ajustes necesarios (consulte Propiedades de configuración de archivo (ver "Propiedades Configuración de archivo" en la página 93)).
4. **Haga clic en OK (aceptar)**.

Conectar un dispositivo o grupo de dispositivos a un almacenamiento

Una vez que un área de almacenamiento está configurada para un servidor de grabación, puede habilitarlo para dispositivos individuales, tales como cámaras, micrófonos o altavoces o un grupo de dispositivos. También puede seleccionar cuál de las áreas de almacenamiento de un servidor de grabación que desea utilizar para el dispositivo individual o de grupo.

1. Expandir **Dispositivos** y seleccione **Cámaras**, **micrófonos** o **altavoces** según sea necesario.
2. Seleccione el dispositivo o grupo de dispositivos.
3. Seleccione la pestaña **registro**.
4. En el área de **Almacenamiento**, seleccione **Seleccionar**.
5. En el cuadro de diálogo que aparece, seleccione la base de datos que se deben almacenar las grabaciones del dispositivo y haga clic en **OK**.
6. En la barra de herramientas, haga clic en **Guardar**.

Al hacer clic en el número de uso del dispositivo para el área de almacenamiento en la ficha Almacenamiento del servidor de grabación, el dispositivo es visible en el informe de mensaje que aparece.

Editar configuración de un dispositivo de almacenamiento o archivo seleccionado

1. Para editar un almacenamiento, seleccione su base de datos de grabación en la lista **Configuración de grabación y archivado**. Para editar un archivo, seleccione la base de datos de archivado.
2. Haga clic en el botón **Editar almacenamiento de grabación**  situado debajo del **Configuración de grabación y archivado** lista.
3. O bien editar una base de datos de registro o editar un archivo.

Si cambia el tamaño máximo de una base de datos, las grabaciones de auto-archivos de sistema que superar el nuevo límite. Se auto-archivos de las grabaciones al archivo siguiente o elimina ellas dependiendo de la configuración de archivado.

Habilitar firma digital para exportación

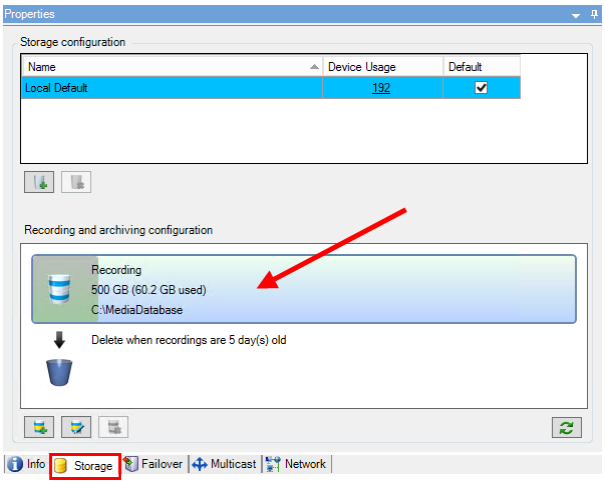
Funcionalidad disponible depende del sistema que está utilizando. Ver tabla de comparación de productos (en la página 24) para más información.

Puede habilitar la firma digital para el video grabado, para que los usuarios del cliente puedan verificar que el video grabado no ha sido manipulado desde que fue grabado. Verificando la autenticidad del video es algo que hace el usuario en XProtect Smart Client – Player después de exportar el video.

La firma también debe activarse en XProtect Smart Client en el diálogo **Exportar**. De lo contrario, el botón **Verificar firmas** en XProtect Smart Client – Player no se muestra.

1. En el panel **Navegación del sitio**, expanda el nodo **Servidores**.

2. Haga clic en **servidores de grabación**.
3. En el panel de vista general, haga clic en el servidor de grabación para el que desea activar la firma.
4. En la parte inferior del panel **Propiedades**, haga clic en la ficha **Almacenamiento**.



5. En la sección **Configuración de grabación y archivo**, haga doble clic en la barra horizontal que representa la base de datos de grabación. Aparece la ventana **Configuración de almacenamiento y grabación**.
6. Seleccione la casilla de verificación **Firma**.
7. Haga clic en **OK** (aceptar).

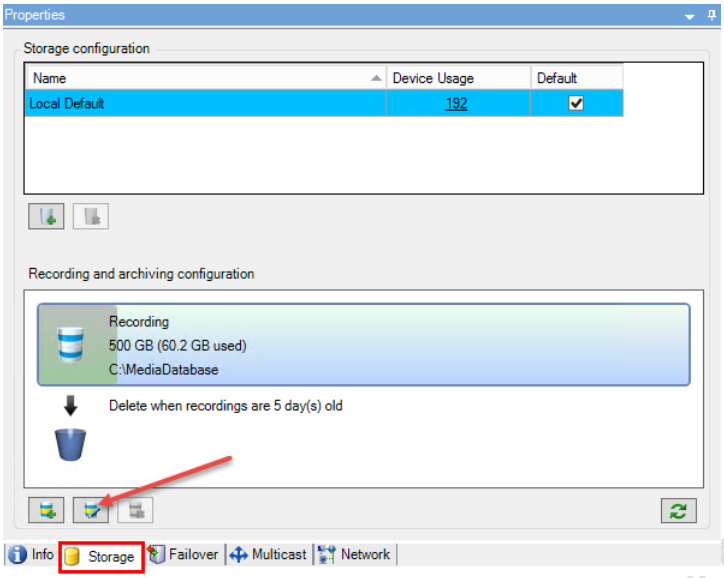
Encripta tus grabaciones

Funcionalidad disponible depende del sistema que está utilizando. Ver tabla de comparación de productos (en la página 24) para más información.

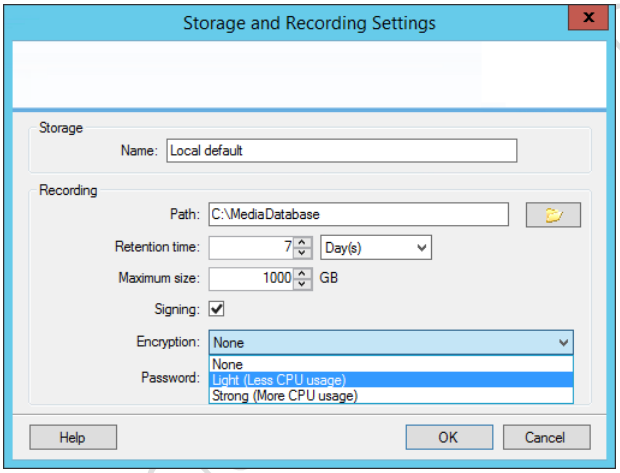
Puede proteger sus grabaciones habilitando el cifrado en el almacenamiento y los archivos de sus servidores de grabación. Puede elegir entre encriptación ligera y fuerte. Cuando habilita el cifrado, también debe especificar una contraseña relacionada.

Advertencia: Permitir o cambiar la configuración de cifrado o la contraseña puede llevar mucho tiempo, dependiendo del tamaño de la base de datos y el rendimiento de la unidad. Puede seguir el progreso en **Tareas actuales**.
No pares el servidor de grabación mientras esta tarea está en curso.

1. Haga clic en el botón **Editar almacenamiento de grabación** debajo de lista **Configuración de grabación y archivado**.



2. En el cuadro de diálogo que aparece, especifique el nivel de encriptación.



3. Se lo dirige automáticamente al cuadro de diálogo **Establecer contraseña** . Ingrese la contraseña y haga clic en **Aceptar**.

Copia de seguridad de grabaciones archivados

Muchas organizaciones desean copias de seguridad de sus grabaciones mediante el uso de unidades de cinta o similar. Exactamente cómo se hace esto es muy individual y depende de los medios de copia de seguridad utilizados en su organización. Sin embargo, lo que sigue es importante tener en cuenta:

Copias de seguridad de archivos en lugar de las bases de datos de la cámara

Siempre debe crear copias de seguridad basadas en el contenido de los archivos, no se basa en bases de datos individuales de la cámara. Si crea copias de seguridad basadas en el contenido de las bases de datos individuales de la cámara, puede causar violaciónes de intercambio u otros fallos.

Al programar una copia de seguridad, asegúrese de que la tarea de respaldo no se superponga con sus tiempos de archivado especificados. Para ver el archivo de calendario de cada servidor de grabación en cada una de las áreas de almacenamiento de un servidor de grabación, consulte la ficha Almacenamiento.

Conocer la estructura de su archivo para que pueda orientar las copias de seguridad

Al archivar las grabaciones, los almacena en una cierta estructura subdirectorio dentro del archivo.

Durante todo el uso regular de su sistema, la estructura sub-directorio es completamente transparente para los usuarios del sistema cuando navegan todas las grabaciones con el XProtect Smart Client. Esto es cierto tanto con grabaciones archivadas y no archivados. Es relevante conocer la estructura sub-directorio si desea realizar una copia de seguridad de sus grabaciones archivadas. Ver Estructura del archivo (explicado) (en la página 89) y Copia de seguridad y restauración de la configuración (ver "Copia de seguridad y restauración de la configuración del sistema" en la página 449).

Estructura del archivo (explicado)

Al archivar las grabaciones, que se almacenan en una cierta estructura subdirectorio dentro del archivo.

Durante todo el uso regular de su sistema, la estructura sub-directorio es completamente transparente para los usuarios del sistema, ya que navegar todas las grabaciones con el XProtect Smart Client con independencia de que las grabaciones se archivan o no. Conocer la estructura de subdirectorio es sobre todo interesante si desea realizar una copia de seguridad de sus grabaciones archivadas.

En cada uno de los directorios de archivos del servidor de grabación, el sistema crea automáticamente subdirectorios independientes. Estos subdirectorios se nombran después del nombre del dispositivo y la base de datos de archivado.

Debido a que puede almacenar grabaciones de diferentes cámaras en el mismo archivo, y desde el archivado para cada cámara es probable que se realiza a intervalos regulares, también se añaden automáticamente nuevos subdirectorios.

Estos subdirectorios cada uno representan aproximadamente el valor de las grabaciones de una hora. La división de una hora hace que sea posible eliminar tan sólo relativamente pequeñas partes de los datos de un archivo si se alcanza el tamaño máximo permitido del archivo.

Los subdirectorios llevan el nombre del dispositivo, seguido de una indicación de dónde provienen las grabaciones (almacenamiento Edge o vía SMTP), **más** la fecha y hora del registro más reciente de la base de datos contenido en el subdirectorio.

Nombrando estructura:

```
...[Ruta de almacenamiento]\[Nombre de almacenamiento]\[nombre-dispositivo] -
 Más fecha y hora de la grabación más reciente] \
```

Si desde el almacenamiento edge:

```
...[Storage Path]\[nombre de almacenamiento]\[nombre-dispositivo] (Edge) -
además de la fecha y hora de la grabación más reciente]\
```

Si de SMTP:

```
...[Storage Path]\[nombre de almacenamiento]\[nombre-dispositivo] (SMTP) -
además de la fecha y hora de la grabación más reciente]\
```

Ejemplo de la vida real:

```
...F:\OurArchive\Archive1\Camera 1 on Axis Q7404 Video Server(10.100.50.137)
- 2011-10-05T11:23:47+02:00\
```

Subdirectorios:

Se añaden automáticamente aún más subdirectorios. La cantidad y la naturaleza de estos sub-directorios dependen de la naturaleza de las grabaciones reales. Por ejemplo, se añaden varios diferentes subdirectorios si las grabaciones se dividen en secuencias de vista técnico. Este suele ser el caso si ha utilizado la detección de movimiento para activar las grabaciones.

- **Medio**: Esta carpeta contiene los medios de comunicación real que sea vídeo o de audio (no ambos).

- **MotionLevel**: Esta carpeta contiene cuadrículas nivel de movimiento generados a partir de los datos de vídeo utilizando nuestro algoritmo de detección de movimiento. Estos datos permiten al Sistema de búsqueda avanzada en función de XProtect Smart Client hacer búsquedas muy rápidas.
- **Movimiento**: En esta carpeta, el sistema almacena secuencias de movimiento. Una secuencia de movimiento es un segmento de tiempo para el que se ha detectado movimiento en los datos de vídeo. Esta información es, por ejemplo, se utiliza en la línea de tiempo en el XProtect Smart Client.
- **Grabación**: En esta carpeta, el sistema almacena secuencias de grabación. Una secuencia de grabación es un segmento de tiempo para el que no son grabaciones coherentes de datos de medios. Esta información es, por ejemplo, utiliza para trazar la línea de tiempo en el XProtect Smart Client.
- **Firma**: Esta carpeta contiene las firmas generadas para los datos multimedia (en la carpeta Media). Con esta información, puede verificar que los datos de los medios no han sido manipulados desde que se grabaron.

Si desea realizar una copia de seguridad de sus archivos, puede orientar sus copias de seguridad si usted sabe los fundamentos de la estructura subdirectorio.

Ejemplos de copia de seguridad:

Para realizar una copia de seguridad del contenido de un archivo completo, copia de seguridad del directorio de archivo requerido y todo su contenido. Por ejemplo, todo bajo:

```
...F:\OurArchive\
```

Para copias de seguridad de las grabaciones de una cámara en particular a partir de un determinado período de tiempo, haga una copia de seguridad del contenido de los únicos subdirectorios pertinentes. Por ejemplo, todo bajo:

```
...F:\OurArchive\Archive1\Camera 1 on Axis Q7404 Video Server(10.100.50.137)
- 2011-10-05T11:23:47+02:00\
```

Eliminar un archivo desde un dispositivo de almacenamiento

1. Seleccione el archivo de la lista **Configuración de grabación y archivado**.

   Sólo es posible borrar el último archivo de la lista. El archivo no tiene que estar vacío.

2. Haga clic en el  botón situado debajo de la **Configuración de grabación y archivado** lista.
3. Haga clic en **Sí**.

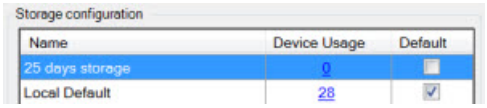
Eliminar un almacenamiento

No se puede eliminar el almacenamiento predeterminado o almacenes que utilizan los dispositivos como el almacenamiento de grabación para grabaciones en vivo.
Esto significa que puede necesitar Mover dispositivos (ver "Mover hardware" en la página 112) y cualquier grabación aún no archivada en otro almacenamiento antes de eliminar el almacenamiento.

1. Para ver la lista de dispositivos que utilizan este almacenamiento, haga clic en el número de uso del dispositivo.

   Si el almacenamiento tiene datos de los dispositivos que se han movido a otro servidor de grabación, aparece una advertencia. Haga clic en el enlace para ver la lista de dispositivos.

2. Siga los pasos Mover grabaciones no archivadas del almacenamiento a otro (ver "Mover grabaciones no archivados de un almacenamiento a otro" en la página 91).
3. Continúe hasta que haya movido todos los dispositivos.
4. Seleccione el almacenamiento que desea eliminar.



5. Haga clic en el  botón situado debajo de la **Configuración de almacenamiento** lista.
6. Haga clic en **Sí**.

Mover grabaciones no archivados de un almacenamiento a otro

Usted se mueve grabaciones de una base de datos de grabación en vivo a otro de la pestaña **registro** del dispositivo.

1. Seleccione el tipo de dispositivo. En el panel **general**, seleccione el dispositivo.
2. Haga clic en la ficha **Registro**. En la parte superior de la zona de **Almacenamiento**, haga clic en **Seleccionar**.
3. En el cuadro de diálogo **Seleccionar almacenamiento**, seleccione la base de datos.
4. **Haga clic en OK (aceptar)**.
5. En el cuadro de diálogo **Acción de grabaciones**, seleccione si desea quitar ya existente - pero **no archivado** - grabaciones para el nuevo almacenamiento o si desea eliminarlos.
6. **Haga clic en OK (aceptar)**.

Propiedades de almacenamiento y configuraciones para la grabación

Funcionalidad disponible depende del sistema que está utilizando. Ver tabla de comparación de productos (en la página 24) para más información.

En la cuadro de diálogo **Configuración de almacenamiento y grabación**, especifique lo siguiente:

Nombre	Descripción
Nombre	Cambie el nombre del almacenamiento, si es necesario. Los nombres deben ser únicos.
Ruta	Especificar la ruta de acceso al directorio en el que guardar las grabaciones en este almacenamiento. El almacenamiento no necesariamente tiene que estar ubicado en el equipo servidor de grabación. Si no existe el directorio, puede crearlo. Las unidades de red se deben especificar utilizando el formato UNC (Convención de nomenclatura universal), ejemplo: \\server\volume\directory\.

Nombre	Descripción
Periodo de retención	Especificar por cuánto tiempo debe permanecer grabaciones en el archivo antes de que se elimine o se mueva al siguiente archivo (dependiendo de la configuración de archivo). El tiempo de retención debe ser siempre mayor que el tiempo de retención del archivo anterior o la base de datos de grabación por defecto. Esto se debe a que el número de días de retención especificado para un archivo incluye todos los períodos de retención indicados anteriormente en el proceso.
Tamaño máximo	Seleccione el número máximo de gigabytes de datos de grabación para guardar en la base de datos de registro. Grabación de datos en exceso de la cantidad especificada de gigabytes es auto-movido al primer archivo en la lista - en su caso se especifica - o eliminados. **Importante**: Cuando hay menos de 5 GB de espacio es libre, el sistema siempre auto-archivos (o elimina si no se define el siguiente archivo) los datos más antiguos en una base de datos. Si es menos de 1 GB de espacio es libre, se eliminan los datos. Una base de datos siempre requiere de 250 MB de espacio libre. Si se alcanza este límite (si los datos no se eliminan suficientemente rápido), no hay más datos se escriben en la base de datos hasta que se haya liberado suficiente espacio. El tamaño máximo real de su base de datos es la cantidad de gigabytes que especifique, menos de 5 GB.
Firma	Permite a una firma digital a las grabaciones. Esto significa, por ejemplo, que el sistema confirma que el vídeo exportado no ha sido modificado o alterado al ser reproducidos. El sistema utiliza el algoritmo SHA-2 para la firma digital.
Cifrado	Seleccione el nivel de cifrado de las grabaciones: • **Ninguno** • **Ligero (menor uso de la CPU)** • **Fuerte (mayor uso de la CPU)** El sistema utiliza el algoritmo AES-256 para el cifrado. Si selecciona **Ligero**, se cifra una parte de la grabación. Si selecciona **Fuerte**, toda la grabación está encriptada. Si elige activar el cifrado, también debe especificar una contraseña a continuación.
Contraseña	Introduzca una contraseña para los usuarios autorizados a ver los datos cifrados. Milestone recomienda que utilice contraseñas seguras. Las contraseñas seguras no contienen palabras que se pueden encontrar en un diccionario o forman parte del nombre del usuario. Incluyen ocho o más caracteres alfanuméricos, mayúsculas y minúsculas y caracteres especiales.

Propiedades Configuración de archivo

En la **configuración de archivo** cuadro de diálogo, especifique lo siguiente:

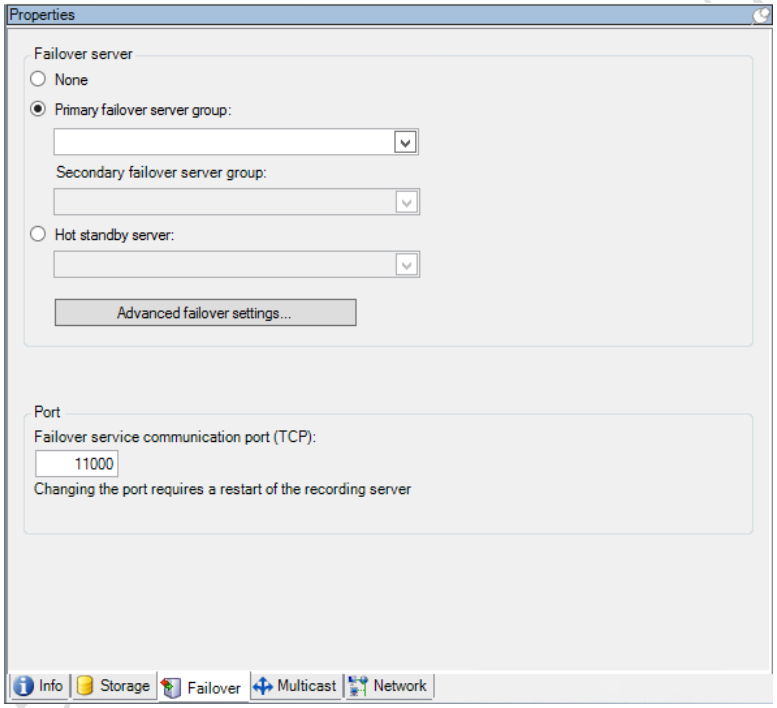
Nombre	Descripción
Nombre	Cambie el nombre del almacenamiento, si es necesario. Los nombres deben ser únicos.
Ruta	Especificar la ruta de acceso al directorio en el que guardar las grabaciones en este almacenamiento. El almacenamiento no necesariamente tiene que estar ubicado en el equipo servidor de grabación. Si no existe el directorio, puede crearlo. Las unidades de red se deben especificar utilizando el formato UNC (Convención de nomenclatura universal), ejemplo: \\server\volume\directory\.
Periodo de retención	Especificar por cuánto tiempo debe permanecer grabaciones en el archivo antes de que se elimine o se mueva al siguiente archivo (dependiendo de la configuración de archivo). El tiempo de retención debe ser siempre mayor que el tiempo de retención del archivo anterior o la base de datos de grabación por defecto. Esto se debe a que el número de días de retención especificado para un archivo incluye todos los períodos de retención indicados anteriormente en el proceso.
Tamaño máximo	Seleccione el número máximo de gigabytes de datos de grabación para guardar en la base de datos de registro. Grabación de datos en exceso de la cantidad especificada de gigabytes es auto-movido al primer archivo en la lista - en su caso se especifica - o eliminados. **Importante**: Cuando hay menos de 5 GB de espacio es libre, el sistema siempre auto-archivos (o elimina si no se define el siguiente archivo) los datos más antiguos en una base de datos. Si es menos de 1 GB de espacio es libre, se eliminan los datos. Una base de datos siempre requiere de 250 MB de espacio libre. Si se alcanza este límite (si los datos no se eliminan suficientemente rápido), no hay más datos se escriben en la base de datos hasta que se haya liberado suficiente espacio. El tamaño máximo real de su base de datos es la cantidad de gigabytes que especifique, menos de 5 GB.
Calendario	Especifique un programa de archivado que resume los intervalos con los que el proceso de archivo debe comenzar. Puede archivar con mucha frecuencia (en principio cada hora durante todo el año), o muy poca frecuencia (por ejemplo, cada primer lunes de cada 36 meses).

Nombre	Descripción
Reducir velocidad de fotogramas	Para reducir FPS al archivar, seleccione la casilla de verificación **Reducir la velocidad de fotogramas** y establecer un cuadro por segundo (FPS). La reducción de velocidades de cuadro por un número seleccionado de FPS hace que sus grabaciones ocupan menos espacio en el archivo, sino que también reduce la calidad de su archivo. MPEG-4/H.264/H.265 reduce automáticamente a los fotogramas clave, como mínimo. 0,1 = 1 cuadro por 10 segundos.

Pestaña failover (servidor de grabación)

Funcionalidad disponible depende del sistema que está utilizando. Ver tabla de comparación de productos (en la página 24) para más información.

Si su organización utiliza servidores de grabación failover, utilice la ficha **Failover** para asignar servidores failover a los servidores de grabación, consulte Propiedades de la ficha de Failover (ver "Propiedades de la ficha failover" en la página 96).



Para obtener más información acerca de los servidores de grabación de conmutación por error, la instalación y los ajustes, los grupos de conmutación por error y sus configuraciones, consulte . Servidores de grabación de conmutación por error (explicado) (ver "Servidores de grabación con conmutación por error (explicado)" en la página 101).

Asignar servidores de grabación failover

En la pestaña **Failover** de un servidor de grabación, puede elegir entre tres tipos de configuraciones de conmutación por error:

- Sin configuración failover
- Una configuración de conmutación por error primaria / secundaria (espera en frío)
- Una configuración de espera activa.

Si selecciona **b** y **c**, debe seleccionar el servidor / grupos específicos. Con **b**, también puede seleccionar un grupo failover secundario. Si el servidor de grabación no está disponible, un servidor de grabación failover del grupo failover primaria se hace cargo. Si también ha seleccionado un grupo failover secundario, un servidor de grabación failover del grupo secundario se hace cargo en caso de todos los servidores de grabación failover en el grupo failover primaria están ocupados. De esta forma, solo corre el riesgo de no tener una solución de conmutación por error en el raro caso en que todos los servidores de grabación failover en el grupo de failover primario, así como en el secundario, estén ocupados.

1. En el panel de **navegación del sitio**, seleccione **Servidores** > **Servidores de grabación**. Esto abre una lista de servidores de grabación.
2. En el panel de **Generalidades**, seleccione el servidor de grabación que desea, entre en la pestaña **Failover**.
3. Para elegir el tipo de configuración de conmutación por error, seleccione entre:
   - **Ninguno**
   - **Grupo de servidores failover principal**/**Grupode servidores failover secundario**
   - **Servidor de reserva en caliente**.

   No se puede seleccionar el mismo grupo failover ya que tanto el grupo de migración primaria y secundaria, ni seleccionar servidores failover regulares ya forman parte de un grupo failover como servidores de reserva en caliente.
4. A continuación, haga clic en **Ajustes avanzados de failover**. Esto abre la ventana **Ajustes avanzados de failover**, enumerando todos los dispositivos conectados al servidor de grabación seleccionado. Si seleccionó **Ninguno**, la configuración de failover avanzada también está disponible. El sistema mantiene todas las selecciones para configuraciones de failover posteriores.
5. Para especificar el nivel de soporte de conmutación por error, seleccione **Asistencia completa**, **Sólo en vivo** o **Deshabilitado** para cada dispositivo de la lista. **Haga clic en OK (aceptar)**.
6. En el campo **Puerto de comunicación del servicio de failover (TCP)** editar el número de puerto si es necesario.

Si habilita la compatibilidad de conmutación por error y el servidor de grabación está configurado para seguir funcionando si un almacenamiento de grabación no está disponible, el servidor de grabación failover no se hará cargo. Para que funcione la compatibilidad de conmutación por error, debe seleccionar opción **Detener el servidor de grabación si no hay disponible un almacenamiento de grabación** en la ficha **Almacenamiento** .

Propiedades de la ficha failover

Nombre	Descripción
Ninguno	Seleccione una configuración sin servidores de grabación con conmutación por error.
/ Grupo failover Sever Secundaria grupo de servidores failover primaria	Seleccione una configuración regular failover con una primaria y, posiblemente, un grupo de servidores failover secundario.
Servidor de reserva en caliente	Seleccione una configuración de espera activa con un solo servidor de grabación dedicado como servidor de reserva en caliente.
Ajustes avanzados de failover	Abre la ventana **Ajustes avanzados de failover**. • **Soporte completo**; Habilita la compatibilidad de conmutación por error completa del dispositivo. • **Solo en vivo**: Habilita únicamente la compatibilidad de conmutación por error para las transmisiones en directo en el dispositivo. • **Deshabilitado**: Deshabilita la compatibilidad con la conmutación por error del dispositivo.
Puerto de comunicación del servicio failover (TCP)	Por defecto, el número de puerto es 11000. Se utiliza este puerto para la comunicación entre los servidores de grabación y los servidores de grabación failover. Si cambia el puerto, el servidor de grabación **debe** estar en ejecución y **debe** conectarse al servidor de gestión.

Pestaña de multidifusión (servidor de impresión)

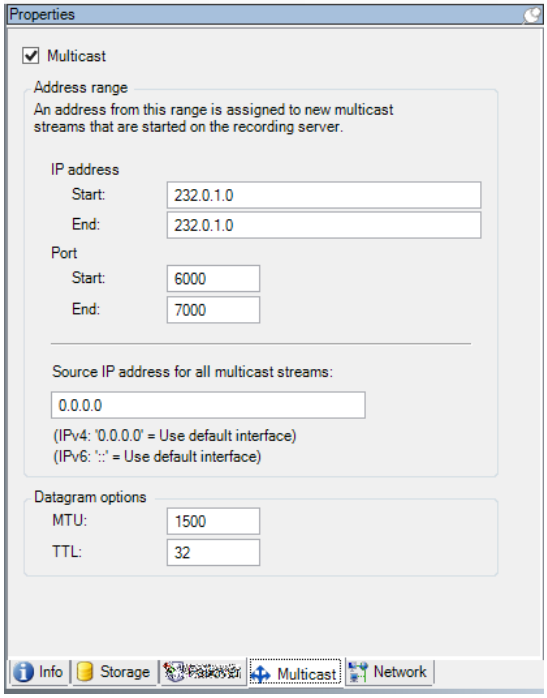
El sistema admite la multidifusión de secuencias en vivo desde servidores de grabación. Si varios usuarios XProtect Smart Client quieren ver vídeo en directo desde la misma cámara, la multidifusión ayuda a ahorrar considerables recursos del sistema. Multidifusión es particularmente útil si tiene funcionalidad Matrix donde varios clientes precisan vídeo en directo desde la misma cámara.

Multidifusión solo es posible para flujos en directo, no para vídeo/audio grabado.

Si el servidor de impresión tiene más de una tarjeta de interfaz de red, sólo es posible utilizar multidifusión en una de ellas. A través del Management Client puede especificar cuál utilizar.

Si está utilizando servidores de conmutación por error, recuerde también especificar la dirección IP de la tarjeta de interfaz de red en los servidores de conmutación por error (ver "Pestaña de multidifusión (servidor de conmutación por error)" en la página 108).

La implementación exitosa de multidifusión también requiere que se haya configurado el equipo de red para retransmitir paquetes de datos de multidifusión para el grupo requerido de sólo destinatarios. Si no, la multidifusión no puede ser diferente de la radiodifusión, lo que puede ralentizar considerablemente la comunicación de red.



Multicasting (explicado)

En la comunicación de red regular, cada paquete de datos es enviado desde un único emisor a un único receptor - un proceso conocido como unidifusión. Pero con la multidifusión puede enviar un único paquete de datos (desde un servidor) a varios destinatarios (clientes) dentro de un grupo. La multidifusión puede ayudar a ahorrar ancho de banda.

- Cuando se utiliza la **unidifusión**, la fuente debe transmitir un flujo de datos para cada destinatario.
- Cuando se utiliza la **multidifusión**, sólo se requiere un único flujo de datos en cada segmento de la red.

Multidifusión como se describe aquí es **no** el streaming de vídeo de la cámara a los servidores, pero a partir de servidores a los clientes.

Con la multidifusión, se trabaja con un grupo de destinatarios definida, basado en opciones tales como rangos de direcciones IP, la posibilidad de habilitar multidifusión / desactivar para cámaras individuales, la capacidad de definir mayor tamaño de paquete de datos aceptables (MTU), el número máximo de routers un paquete de datos debe ser enviada entre (TTL), y así sucesivamente.

La multidifusión no se debe confundir con la **difusión**, que envía los datos a todo el mundo conectado a la red, incluso si los datos no son quizá relevante para todo el mundo:

Nombre	Descripción
Unidifusión	Envía datos desde una única fuente a un único destinatario.
La multidifusión	Envía datos desde una única fuente a varios destinatarios dentro de un grupo claramente definido.

Nombre	Descripción
Radiodifusión	Envía datos desde una única fuente a todo el mundo en una red. Por lo tanto, la radiodifusión puede ralentizar considerablemente la comunicación de red.

Habilitar la multidifusión

Para utilizar la multidifusión, la infraestructura de red debe ser compatible con el estándar IP multidifusión IGMP (Internet Group Management Protocol).

- En la ficha **Multidifusión**, seleccione la casilla de verificación **Multidifusión**.

Si todo el rango de direcciones IP para multidifusión ya está en uso en uno o más servidores de grabación, primero suelte algunas direcciones IP de multidifusión para poder habilitar la multidifusión en los servidores de grabación adicionales.

Asignar rango de direcciones IP

Especificar el intervalo que desea asignar como direcciones para las secuencias de multidifusión desde el servidor de grabación seleccionado. Los clientes se conectan a estas direcciones cuando los usuarios ver el vídeo de multidifusión desde el servidor de grabación.

Para cada fuente de la cámara de multidifusión, la dirección IP y combinación de puerto deben ser únicos (IPv4 ejemplo: 232.0.1.0:6000). Se puede utilizar ya sea una dirección IP y muchos puertos, o muchas direcciones IP y menos puertos. Por defecto, el sistema sugiere una única dirección IP y una serie de puertos de 1000, pero esto se puede cambiar según sea necesario.

Direcciones IP de multidifusión deben estar dentro del rango definido para la asignación dinámica de host por IANA. IANA es la autoridad que supervisa la asignación global de direcciones IP.

Nombre	Descripción
Dirección IP	En el campo **Iniciar**, especifique la primera dirección IP en el rango requerido. A continuación, especifique la última dirección IP del intervalo en el campo **Final**.
Puerto	En el campo **Iniciar**, especifique el primer número de puerto en el rango requerido. A continuación, especifique el último número de puerto en el rango en el campo **Final**.
Dirección IP de origen para todas las secuencias de multidifusión	Sólo se puede multidifusión en una tarjeta de interfaz de red, por lo que este campo es relevante si el servidor de impresión tiene más de una tarjeta de interfaz de red o si tiene una tarjeta de interfaz de red con más de una dirección IP. Para utilizar la interfaz por defecto del servidor de grabación, deje el valor 0.0.0.0 (IPv4) o :: (IPv6) en el campo. Si desea utilizar otra tarjeta de interfaz de red o una dirección IP diferente en la misma tarjeta de interfaz de red, especifique la dirección IP de la interfaz requerida. • IPv4: 224.0.0.0 a 239.255.255.255. • IPv6, la gama se describe en el sitio web IANA (http://www.iana.org).

Especificar las opciones de datagramas

Especificar la configuración de paquetes de datos (datagramas) transmitidos a través de la multidifusión.

Nombre	Descripción
MTU	Unidad de transmisión máxima, el mayor tamaño permitido de paquetes de datos físicos (medido en bytes). Los mensajes más grandes que la MTU especificada se dividen en paquetes más pequeños antes de ser enviados. El valor predeterminado es 1500, que es la opción por defecto en la mayoría de los ordenadores Windows y redes Ethernet.
TTL	Período de vida, el mayor número permitido de saltos que un paquete de datos debe ser capaz de viajar antes de que sea eliminado o devuelto. Un salto es un punto entre dos dispositivos de red, típicamente un router. El valor por defecto es 128.

Habilitar la multidifusión para cámaras individuales

La multidifusión sólo funciona cuando se habilita para las cámaras requeridas:

1. Seleccione el servidor de grabación y seleccione la cámara deseada en el panel **general**.
2. En la ficha **Cliente**, seleccione la casilla de verificación **Multidifusión en directo**. Repita este procedimiento para todas las cámaras requeridas.

Pestaña de red (servidor de impresión)

Se define la dirección IP pública de un servidor de grabación en la pestaña **red**.

¿Por qué utilizar una dirección pública?

Cuando un cliente de acceso, tales como XProtect Smart Client, se conecta a un sistema de vigilancia, una cantidad de la comunicación inicial de datos, incluido el intercambio de direcciones de contacto, se comparte en el fondo. Esto sucede automáticamente, y es completamente transparente para los usuarios.

Los clientes pueden conectarse desde la red local, así como a través de Internet, y en ambos casos el sistema de vigilancia deben proporcionar direcciones adecuadas por lo que los clientes pueden acceder a video en directo y grabado desde los servidores de grabación:

- Cuando los clientes se conectan a nivel local, el sistema de vigilancia debe responder con las direcciones locales y números de puerto.
- Cuando los clientes se conectan a través de Internet, el sistema de vigilancia debe responder con la dirección pública del servidor de grabación. Esta es la dirección del firewall o router NAT (Network Address Translation), y con frecuencia también un número de puerto diferente. La dirección y el puerto a continuación, pueden ser enviados a la dirección y el puerto local del servidor.

  Para facilitar el acceso al sistema de vigilancia desde fuera de un firewall NAT (Network Address Translation), puede utilizar direcciones públicas y el reenvío de puertos. Esto permite a los clientes de fuera del firewall para conectarse a servidores de grabación sin necesidad de utilizar VPN (Virtual

Private Network). Cada servidor de grabación se puede asignar a un puerto específico y el puerto puede ser reenviado por el firewall a la dirección interna del servidor.

Definir la dirección pública y el puerto

1. Para habilitar el acceso del público, seleccione la casilla de verificación **Habilitar acceso público**.
2. Definir la dirección pública del servidor de grabación. Introduzca la dirección del firewall o enrutador NAT para que los clientes que acceden al sistema de vigilancia de Internet pueden conectarse a los servidores de grabación.
3. Especificar un número de puerto público. Siempre es una buena idea que los números de puerto utilizados en el firewall o router NAT son diferentes de las que se utilizan a nivel local.

Si utiliza el acceso del público, configurar el firewall o router NAT así que las peticiones enviadas a la dirección pública y el puerto se reenvían a la dirección local y el puerto de servidores de grabación pertinentes.

Asignar rangos IP locales

Se define una lista de rangos de IP locales, que el sistema de vigilancia debe reconocer como procedentes de una red local.

- En la ficha **Red**, haga clic en **Configurar**.

Retirar un servidor de grabación

Importante: Si elimina un servidor de grabación, se quita toda la configuración especificada en el Management Client para el servidor de grabación, incluido **todo** el hardware asociado del servidor de grabación (cámaras, dispositivos de entrada, etc.).

1. Haga clic con el servidor de grabación que desea eliminar en el panel **general**.
2. Seleccionar **Quitar grabación servidor**.
3. Si está seguro, haga clic en **Yes (sí)**.
4. El servidor de grabación y la totalidad de su hardware asociado se eliminan.

Eliminar todo el hardware en un servidor de grabación

Importante: Cuando se elimina el hardware, todos los datos grabados relacionados con el hardware se eliminan permanentemente.

1. Haga clic con el servidor de grabación en el que desea borrar todo el hardware.
2. Seleccione **Borrar todo el hardware**.
3. Confirmar la eliminación.

Servidores failover

Servidores de grabación con conmutación por error (explicado)

Funcionalidad disponible depende del sistema que está utilizando. Ver tabla de comparación de productos (en la página 24) para más información.

Un servidor de grabación de conmutación por error es un servidor de grabación adicional que toma el relevo del servidor de grabación estándar si éste no está disponible. Puede configurar un servidor de grabación de conmutación por error en dos modos, como **servidor en espera pasiva** o como **servidor en espera activa**.

Se instalan servidores de grabación de conmutación por error como servidores de grabación estándar (ver "Instalar un servidor de grabación failover" en la página 104). Una vez que haya instalado servidores de grabación failover, que son visibles en el Management Client. Milestone recomienda instalar todos los servidores de grabación de conmutación por error en equipos independientes. Asegúrese de que configura servidores de grabación failover con la correcta dirección IP / nombre de host del servidor de gestión y que se compruebe que la cuenta de usuario bajo el cual se ejecuta el servicio de servidor failover tiene acceso a su sistema con derechos de administrador.

Puede especificar qué tipo de apoyo failover que desee en un dispositivo de nivel. Para cada dispositivo en un servidor de grabación, seleccione completo, solamente o ningún apoyo failover vivir. Esto ayuda a priorizar sus recursos failover y, por ejemplo, sólo se estableció failover para el vídeo y no para el audio, o sólo tienen conmutación por error en cámaras esenciales, no en los menos importantes.

Importante: Mientras el sistema está en el modo de conmutación por error, no puede multicast, reemplazar o mover hardware, actualizar el servidor de grabación o cambiar configuraciones de dispositivo como configuración de almacenamiento o configuración de flujo de vídeo.

Servidores de grabación en caso de fallo en frío

En una configuración de servidor de grabación de conmutación por error en espera en frío, agrupe varios servidores de grabación de conmutación por error en un grupo de conmutación por error. Todo el grupo de conmutación por error está dedicado a hacerse cargo de cualquiera de varios servidores de grabación preseleccionados, si uno de ellos no está disponible. Puede crear tantos grupos como desee (ver "Servidores de grabación de conmutación por error de grupo para el modo de espera en frío" en la página 105).

La agrupación tiene un beneficio claro: cuando más adelante se especifica el que la grabación failover servidores deben tomar el relevo de un servidor de grabación, seleccione un grupo de servidores de grabación failover. Si el grupo seleccionado contiene más de un servidor de grabación failover, este le ofrece la seguridad de tener servidor de grabación de más de un servidor de grabación failover listo para hacerse cargo de si un servidor de grabación deja de estar disponible. Puede especificar un grupo de servidores de conmutación por error secundario que tome el control del grupo principal si todos los servidores de grabación del grupo principal están ocupados. Un servidor de grabación de conmutación por error sólo puede ser miembro de un grupo a la vez.

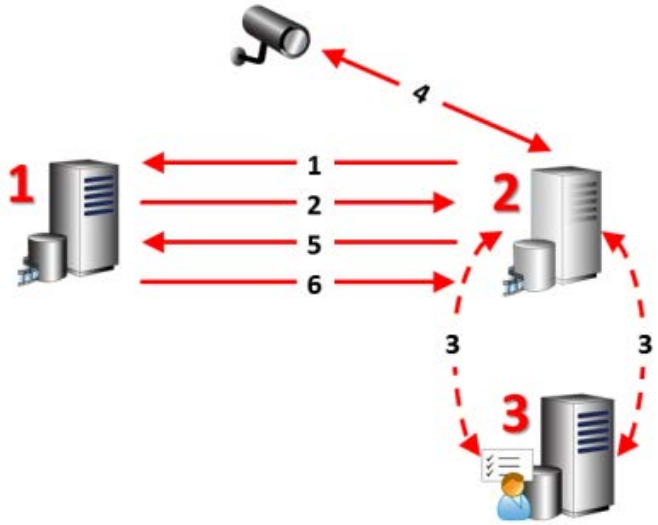
Los servidores de grabación de conmutación por error en un grupo de conmutación por error se ordenan en una secuencia. La secuencia determina el orden en el que los servidores de grabación de conmutación por error tomarán el relevo de un servidor de grabación. De forma predeterminada, la secuencia refleja el orden en el que ha incorporado los servidores de grabación de conmutación por error en el grupo de conmutación por error: first in es el primero de la secuencia. Puede cambiarlo si es necesario.

Servidores de grabación failover de espera activa

En una configuración de servidor de grabación de conmutación por error hot-standby, dedica un servidor de grabación de conmutación por error a tomar de **un solo servidor de grabación**. Debido a esto, el sistema

puede mantener este servidor de grabación de conmutación por error en un modo "en espera", lo que significa que está sincronizado con la configuración correcta / actual del servidor de grabación al que está dedicado y puede tomar mucho más rápido que una grabación de conmutación por error servidor. Como se ha mencionado, se asignan los servidores de reserva en caliente a un servidor de grabación y no podemos grupo de la misma. No puede asignar servidores de conmutación por error que ya formen parte de un grupo de conmutación por error como servidores de grabación de hot stand.

Pasos de conmutación por error (explicados)



Involucrados **servidores** (números en rojo):

1. Servidor de grabación
2. Servidor de grabación failover
3. Servidor de gestión.

Pasos de conmutación por error para **En espera en frío** configuraciones:

1. Para comprobar si está funcionando o no, un servidor de grabación failover tiene una conexión TCP sin parar a un servidor de grabación.
2. Esta conexión se interrumpe.
3. El servidor de grabación failover solicita la configuración actual del servidor de impresión desde el servidor de gestión. El servidor de gestión envía la configuración solicitada, el servidor de grabación failover recibe la configuración, se pone en marcha y empieza a grabar en nombre del servidor de grabación.
4. El servidor de grabación failover y los datos pertinentes de intercambio de vídeo de la cámara (s).
5. El servidor de grabación failover continuamente trata de volver a establecer la conexión con el servidor de grabación.
6. Cuando se restablece la conexión con el servidor de grabación, el servidor de grabación failover se apaga y el servidor de grabación obtiene datos de vídeo (si lo hay) registró durante su tiempo de inactividad y los datos de vídeo se fusiona de nuevo en la base de datos del servidor de grabación.

Pasos failover para configuraciones **Hot Standby**:

1. Para comprobar si está funcionando o no, un servidor de reserva en caliente tiene una conexión TCP sin parar a su servidor de grabación asignado.
2. Esta conexión se interrumpe.

3. Desde el servidor de gestión, el servidor de reserva en caliente ya conoce la configuración actual de su servidor de grabación asignado y comienza a grabar en su nombre.
4. El servidor de reserva en caliente y los datos pertinentes de intercambio de vídeo de la(s) cámara(s).
5. El servidor de reserva en caliente continuamente trata de restablecer la conexión con el servidor de grabación.
6. Cuando se restablece la conexión con el servidor de grabación y el servidor de reserva en caliente vuelve al modo de espera activa, el servidor de grabación obtiene datos de vídeo (si lo hay) registró durante su tiempo de inactividad y los datos de vídeo se fusiona de nuevo en la grabación la base de datos del servidor.

Funcionalidad del servidor de grabación de conmutación por error (explicada)

- Un servidor de grabación de conmutación por error comprueba el estado de los servidores de registro relevantes cada 0,5 segundos. Si un servidor de grabación no contesta dentro de 2 segundos, el servidor de grabación se considera disponible y el servidor de grabación failover se hace cargo.
- Un servidor de conmutación por error espera passiva toma el control del servidor de grabación que se ha quedado inactivo después de cinco segundos, más el tiempo que tarda el servicio Recording Server de iniciar el servidor de conmutación por error de grabación en arrancar y el tiempo que tarda en conectar a las cámaras. Por el contrario, un servidor de grabación de conmutación por error con respaldo en caliente se hace cargo más rápidamente porque el servicio de servidor de grabación ya se está ejecutando con la configuración correcta y sólo tiene que iniciar sus cámaras para entregar alimentaciones. Durante el período de puesta en marcha, se puede almacenar ni grabaciones, ni ver vídeo en directo desde las cámaras afectadas.
- Cuando un servidor de grabación vuelve a estar disponible, automáticamente se hace cargo del servidor de grabación por fallo. Las grabaciones almacenadas por el servidor de grabación con conmutación por error se fusionan automáticamente en las bases de datos del servidor de grabación estándar. El tiempo que tarda la fusión depende de la cantidad de grabaciones, capacidad de la red y más. Durante el proceso de fusión, no puede examinar las grabaciones del período durante el cual el servidor de grabación con conmutación por error se hizo cargo.
- Si un servidor de grabación de conmutación por error tiene que tomar el control de otro servidor de grabación durante el proceso de fusión en una configuración de servidor de grabación de conmutación por error en espera passiva, pospone el proceso de fusión con el servidor de grabación A y toma el relevo del servidor de grabación B. Cuando el servidor de grabación B vuelve a estar disponible , El servidor de grabación de conmutación por error ocupa el proceso de fusión con el servidor de registro A, después de lo cual comienza a fusionarse con el servidor de grabación B.
  En una configuración de espera activa, un servidor de reserva en caliente no puede hacerse cargo de otro servidor de grabación, ya que sólo puede ser de espera activa para un solo servidor de grabación. Pero si ese servidor de grabación vuelve a fallar, la reserva en caliente se hace cargo de nuevo y mantiene las grabaciones del período anterior. El servidor de grabación grabaciones mantiene hasta que se fundan de nuevo a la grabadora primaria o hasta que el servidor de grabación failover se queda sin espacio en disco.
- Una solución failover no proporciona redundancia completa. Sólo puede servir como una manera fiable de reducir al mínimo el tiempo de inactividad. Si un servidor de grabación vuelva a estar disponible, el servicio failover del servidor se asegura de que el servidor de grabación está listo para almacenar grabaciones de nuevo. Sólo entonces es la responsabilidad para almacenar grabaciones transmitidas de vuelta al servidor de grabación estándar. Por lo tanto, una pérdida de grabaciones en esta etapa del proceso es muy poco probable.

- Los usuarios del cliente apenas notan que un servidor de grabación failover se hace cargo. Un breve descanso se produce, por lo general sólo durante unos segundos, cuando el servidor de grabación failover se hace cargo. Durante esta pausa, los usuarios no pueden acceder a video desde el servidor de grabación afectada. Los usuarios del cliente pueden reanudar la visualización de vídeo en directo tan pronto como el servidor de grabación failover se ha hecho cargo. Debido a recientes grabaciones se almacenan en el servidor de grabación failover, pueden reproducir las grabaciones después el servidor de grabación failover se hizo cargo. Los clientes no pueden reproducir las grabaciones más antiguas, almacenadas sólo en el servidor de grabación afectada hasta que el servidor de grabación está funcionando de nuevo y se ha hecho cargo del servidor de grabación failover. No se puede acceder a las grabaciones archivadas. Cuando el servidor de grabación está funcionando de nuevo, un proceso de fusión se lleva a cabo durante el cual las grabaciones failover se fusionan de nuevo en la base de datos del servidor de grabación. Durante este proceso, no se puede reproducir grabaciones a partir del período durante el cual el servidor de grabación failover se hizo cargo.
- En una configuración en espera en frío, no es necesario configurar un servidor de grabación de conmutación por error como copia de seguridad para otro servidor de grabación con conmutación por error. Esto se debe a que no se asignan determinados servidores de grabación failover para asumir el control de un servidor de grabación estándar. En su lugar, se puede asignar grupos failover. Un grupo failover debe contener la grabación de al menos un servidor failover, pero se puede añadir tantos servidores de grabación failover, según sea necesario. Proporcionado un grupo failover contiene más de un servidor de grabación de failover, más de un servidor de grabación failover puede tomar el relevo. En una configuración de espera activa, no se puede establecer un registro de los servidores failover o servidores de reserva en caliente para un servidor de reserva en caliente.

Instalar un servidor de grabación failover

Importante: Durante el proceso de instalación se le pedirá que especifique una cuenta de usuario en la que se ejecutará el **servicio Failover Server**. Esta cuenta de usuario debe poseer derechos de administrador en el sistema. Tenga en cuenta también que si ejecuta grupos de trabajo debe ignorar las pautas de instalación normales para los servidores de grabación y usar el método de instalación alternativa para grupos de trabajo.

Cuando haya instalado el servidor de gestión usando el instalador común, puede descargar el instalador del servidor de grabación independiente desde la página web del servidor de gestión. Como parte de este instalador, puede especificar si el instalador debe resultar en un servidor de grabación estándar o un servidor de grabación failover.

1. Entre en la página web de descargas del servidor de gestión y seleccione el instalador de Recording Server adecuado. Guarde el instalador en un lugar apropiado y ejecútelo directamente desde la página web.
2. Seleccione el **Idioma** que quiere usar durante la instalación. Haga clic en **Continuar**.
3. De la lista de selección, seleccione **Failover** para instalar un servidor de grabación como servidor de grabación failover.
4. Especifique las propiedades del servidor de grabación failover. Haga clic en **Continuar**.
5. Cuando instale un servidor de grabación failover es necesario que use una cuenta de usuario particular nombrada **Esta cuenta**. Si es necesario, introduzca una contraseña y confírmela. Haga clic en **Continuar**.
6. Seleccione **Ubicación de los archivos** para el archivo del programa. En **Idioma del producto**, seleccione el idioma en que quiere instalar su sistema. Haga clic en **Install** (instalar).
7. El software se instala. Cuando haya terminado, verá una lista de los componentes instalados correctamente. Haga clic en **Cerrar**.

Cuando haya instalado el servidor de grabación failover, puede comprobar su estado desde el icono de **servicio de servidor failover**.

Configurar y habilitar servidores de grabación failover

Importante: Si ha deshabilitado el servidor de grabación failover, debe habilitarlo antes de que pueda tomar el control de los servidores de grabación estándar.

Haga lo siguiente para habilitar un servidor de grabación failover y edite sus propiedades básicas:

1. En el panel **Navegación del sitio** , seleccione **Servidores** > **Servidores failover**. Esto abre una lista de servidores failover de grabación instaladas y los grupos failover.
2. En el panel **Descripción general**, seleccione el servidor de grabación failover requerido.
3. Haga clic con el botón derecho y seleccione **Habilitado**. El servidor de grabación failover ahora está habilitado.
4. Para editar las propiedades del servidor de grabación failover, vaya a la pestaña **Información**.
5. Cuando termine, vaya a la pestaña **de la red** . Aquí puede definir la dirección IP pública del servidor de grabación failover y más. Esto es relevante si usa NAT (Traducción de direcciones de red) y reenvío de puertos. Consulte la pestaña **Red** del servidor de grabación estándar para obtener más información.
6. En el panel de **navegación del sitio**, seleccione **Servidores** > **Servidores de grabación**. Seleccione el servidor de grabación para el que desea soporte de failover y asigne servidores de grabación failover (ver "Asignar servidores de grabación failover " en la página 95).

Para ver el estado de un servidor de grabación failover, mantenga el mouse sobre el ícono de la bandeja Failover Recording Server Manager en el área de notificación. Aparece una información sobre herramientas que contiene el texto ingresado en el campo Descripción del servidor de grabación failover. Esto puede ayudarlo a determinar de qué servidor de grabación está configurado el servidor de grabación failover para sustituirlo.

Importante: El servidor de grabación failover hace ping al servidor de administración regularmente para verificar que esté en línea y pueda solicitar y recibir la configuración de los servidores de grabación estándar cuando sea necesario. Si bloquea el ping, el servidor de grabación failover no puede tomar el control de los servidores de grabación estándar.

Servidores de grabación de conmutación por error de grupo para el modo de espera en frío

1. Seleccione **Servidores** > **Servidores de conmutación por error**. Esto abre una lista de servidores failover de grabación instaladas y los grupos failover.
2. En el panel **general**, haga clic en el nodo superior **Grupos failover** y seleccione **Añadir grupo**.
3. Especifique un nombre (en este ejemplo Grupo Failover 1) y una descripción (opcional) de su nuevo grupo. **Haga clic en OK (aceptar)**.
4. Haga clic con el botón secundario en el grupo (Failover Group 1) que acaba de crear. Seleccione **Editar miembros de grupo**. Esto abre la ventana **Seleccione miembros de grupos**.
5. Arrastrar y soltar o utilizar los botones para mover el servidor de grabación failover seleccionado (s) del lado izquierdo al lado derecho. Haga clic en **OK**. El servidor de grabación failover seleccionado (s) ahora pertenece al grupo (Grupo 1 failover) que acaba de crear.
6. Vaya a la pestaña **Secuencia**. Haga clic **Arriba** y **Abajo** para establecer la secuencia interna de los servidores regulares grabaciones failover en el grupo.

Leer los iconos de estado del servidor de grabación failover

Los siguientes iconos representan el estado de los servidores de grabación failover (iconos son visibles en el panel **general**):

Icono	Descripción
	El servidor de grabación failover o bien se espera o "ver". Cuando la espera, el servidor de grabación failover no está configurado para tomar el relevo de cualquier servidor de grabación todavía. Cuando "ver", el servidor failover de grabación está configurado para ver uno o más servidores de grabación.
	El servidor de grabación failover se ha hecho cargo del servidor de grabación designada. Si coloca el cursor sobre el icono del servidor, se ve una información sobre herramientas. Utilice la información de herramientas para ver qué servidor de grabación del servidor de grabación failover se ha hecho cargo de.
	La conexión con el servidor de grabación failover se ha roto.

Las propiedades del servidor de grabación failover

Especificar las siguientes propiedades del servidor de grabación failover:

Nombre	Descripción
Nombre	El nombre del servidor de grabación failover tal como aparece en el Management Client, registros y mucho más.
Descripción	Un campo opcional que se puede utilizar para describir el servidor de grabación failover, por ejemplo, que la grabación del servidor que toma el relevo de.
Nombre de host	Muestra la dirección de red del servidor de grabación failover. No se puede cambiar esto.
Puerto UDP	El número de puerto utilizado para la comunicación entre servidores de grabación failover. El puerto predeterminado es 8844.
Ubicación de la base	Especifique la ruta a la base de datos utilizada por el servidor de grabación failover para el almacenamiento de grabaciones. No se puede cambiar la ruta de la base de datos, mientras que el servidor de grabación failover toma el relevo de un servidor de grabación. El sistema aplica los cambios cuando el servidor de grabación failover ya no está tomando el relevo de un servidor de grabación.
Habilitar este servidor failover	Borrar para desactivar el servidor de grabación failover (seleccionado por defecto). Tenga en cuenta que debe deshabilitar servidores de grabación failover antes de que puedan tomar el relevo de servidores de grabación.

Propiedades del grupo failover

Pestaña **Información**:

Campo	Descripción
Nombre	El nombre del grupo failover tal como aparece en el Management Client, registros y mucho más.
Descripción	Una descripción opcional, por ejemplo la ubicación física del servidor.

Pestaña **secuencia**:

Campo	Descripción
Especificar la secuencia de failover	Utilizar **Hasta** y **hacia abajo** para establecer la secuencia deseada de servidores de grabación failover regulares dentro del grupo.

Servicios de servidor de grabación de conmutación por error (explicado)

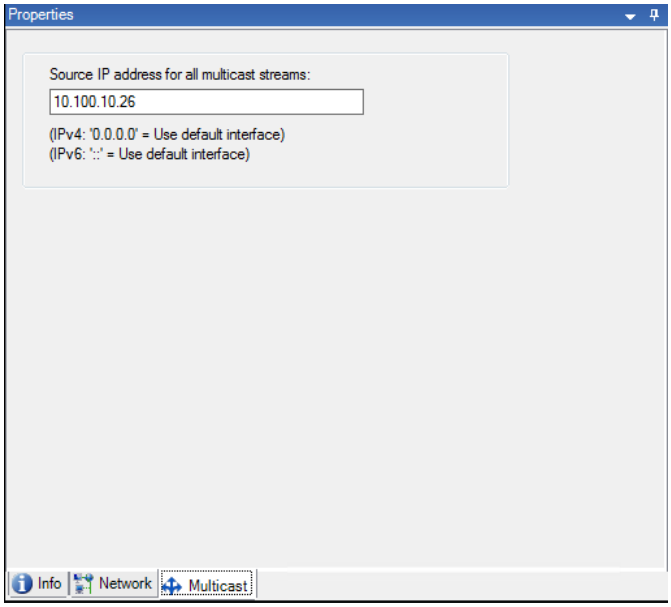
Un servidor de grabación failover ha instalado dos servicios:

- Un servicio de servidor failover, que se ocupa de los procesos de tomar el relevo de servidor de grabación. Este servicio siempre se está ejecutando, y comprueba constantemente el estado de los servidores de grabación en cuestión.
- Un servicio de servidor failover de grabación, lo que permite al servidor de grabación failover para actuar como un servidor de grabación.

  En una configuración en espera en frío, este servicio sólo se inicia cuando es necesario, es decir, cuando el servidor de grabación en caso de fallo de reposo en frío toma el control del servidor de grabación. A partir de este servicio suele tardar un par de segundos, pero puede tomar más tiempo, dependiendo de la configuración de seguridad locales y mucho más.
  En una configuración de espera activa, este servicio siempre se está ejecutando, permitiendo que el servidor espera activa asuma el control más rápido que el servidor de grabación en caso de fallo en espera passiva.

Pestaña de multidifusión (servidor de conmutación por error)

Si utiliza servidores de conmutación por error y ha habilitado la multidifusión de transmisión en vivo, debe especificar la dirección IP de la tarjeta de interfaz de red que está utilizando, tanto en los servidores de grabación como en los servidores de conmutación por error.



Para obtener más información acerca de la multidifusión, consulte Multicasting (explicado) (en la página 97) o Pestaña de multidifusión (servidor de grabación) (ver "Pestaña de multidifusión (servidor de impresión)" en la página 96).

Ver mensajes de estado

1. En el servidor de grabación failover, haga clic en el icono **servicio Milestone Failover Server**.
2. Seleccione **Mostrar mensajes de estado**. Aparece el **servidor de mensajes de estado failover** ventana con una lista mensajes de estado con fecha y hora.

Cambiar la dirección del servidor de gestión

El servidor de grabación failover debe ser capaz de comunicarse con el servidor de gestión del sistema. Se especifica la dirección IP / nombre de host del servidor de gestión durante la instalación del servidor de grabación failover. Si desea cambiar la dirección del servidor de gestión, haga lo siguiente:

1. En el servidor failover de grabación, detener el servicio de servidor failover de grabación.
2. Haga clic en el icono del área de notificación de servizio Failover Recording Server de nuevo.
3. Seleccione **Cambie la configuración**. Aparece la configuración de grabación failover **Server** ventana, por lo que puede especificar la dirección IP o el nombre de host del servidor de gestión con la que el servidor de grabación failover debe comunicarse.

Ver información de versión

Conocer la versión exacta de su **servicio failover del servidor de grabación** es una ventaja si se necesita, con soporte técnico.

1. En el servidor de grabación failover, haga clic en el icono de servicio **Milestone Failover Recording Serve**.

2. Seleccionar **Sobre**.
3. Un pequeño cuadro de diálogo se abre que muestra la versión exacta de su **servicio Failover Recording Server**.

Hardware y servidores remotas

Hardware (explicado)

Hardware representa o bien:

- La unidad física que se conecta directamente al servidor de grabación del sistema de vigilancia a través de IP, por ejemplo una cámara, un codificador de vídeo, un módulo de E / S o,
- Un servidor de grabación en un sitio remoto en una configuración de Milestone Interconnect.

Consulte Añadir hardware (en la página 109) para leer acerca de cómo añadir hardware a su sistema.

Añadir hardware

Tiene varias opciones para añadir hardware para cada servidor de grabación que usted ha autorizado en su sistema.

Importante: Si el hardware se encuentra detrás de un router NAT habilitado o un servidor de seguridad, es posible que tenga que especificar un número de puerto diferente y configurar el router / firewall para que se asigna el puerto y direcciones IP que el hardware utiliza.

El **asistente Añadir hardware** le ayuda a detectar hardware como cámaras y codificadores de vídeo en su red y añadirlos a los servidores de grabación de su sistema. El asistente también le ayuda a añadir servidores de grabación remotos para configuraciones de Milestone Interconnect. Añadir hardware de sólo **un servidor grabación** a la vez.

1. Para acceder para **Añadir hardware**, haga clic en el servidor de grabación deseada y seleccione **Añadir hardware**.
2. Seleccione una de las opciones del asistente (ver a continuación) y siga las instrucciones en la pantalla.
3. Después de la instalación, se puede ver el hardware y que esté dispositivos en el panel **general**.

Nombre	Descripción
Expreso (Recomendado)	El sistema busca automáticamente el nuevo hardware de la red local del servidor de grabación. Seleccione lacasilla de verificación **Mostrar el hardware que se ejecutan en otros servidores de grabación** para ver si hardware detectado se está ejecutando en otros servidores de grabación. Puede seleccionar esta opción cada vez que añada un nuevo hardware de su red y desea utilizarlo en su sistema. No se puede utilizar esta opción para añadir sistemas remotos en configuraciones de Milestone Interconnect.

Nombre	Descripción
Escaneo rango de direcciones	El sistema escanea la red para la hardware correspondiente y sistemas remotos Milestone Interconnect basados en sus especificaciones de: • Hardware de los nombres de usuario y contraseñas. No es necesario si su hardware utiliza los nombres de usuario y contraseñas por defecto de fábrica. • controladores • rangos de IP (sólo IPv4) • número de puerto (por defecto = 80) Puede seleccionar esta opción cuando sólo se desea escanear una parte de su red, por ejemplo, cuando se expande el sistema.
Manual	Especificar los detalles de cada hardware y de sistemas remotos Milestone Interconnect separado. Esto puede ser una buena opción si desea añadir sólo unas pocas piezas de hardware, y usted sabe que sus direcciones IP, nombres de usuario y contraseñas correspondientes o si una cámara no es compatible con la función de descubrimiento automático.
Hardware de conexión remota	Las exploraciones del sistema para el hardware conectado a través de un servidor conectado de forma remota. Puede usar esta opción si ha instalado servidores para, por ejemplo, la conexión de la cámara Axis One-click. No se puede utilizar esta opción para añadir sistemas remotos en configuraciones de Milestone Interconnect.

Desactivar / activar el hardware

Hardware adicional es **activada** de forma predeterminada.

Se puede ver si el hardware está activado o desactivado de esta manera:

Habilitado
Discapacitado

Para desactivar el hardware adicional, por ejemplo, a efectos de licencia o de rendimiento:

1. Expanda el servidor de grabación, haga clic en el hardware que desea desactivar.
2. Seleccione **Habilitado** para borrar o seleccionarla.

Editar hardware

Puede editar la configuración básica, como el nombre de direcciones IP / host, para el hardware añadido:

1. Expanda el servidor de impresión, haga clic con el hardware que desea editar.

2. Seleccione **Editar hardware**. Esto abre la ventana de **edición de hardware**, donde puede editar las propiedades relevantes.

3. **Haga clic en OK (aceptar)**.

Activar / desactivar dispositivos individuales

Cámaras son de forma predeterminada **habilitado**.

Micrófonos, altavoces, metadatos, entradas y **salidas** son por defecto **discapacitados**.

Esto significa que los micrófonos, altavoces, metadatos, entradas y salidas deben estar habilitadas de forma individual antes de poder utilizarlos en el sistema. La razón de esto es que los sistemas de vigilancia se basan en las cámaras, mientras que el uso de micrófonos y así sucesivamente es muy individual en función de las necesidades de cada organización.

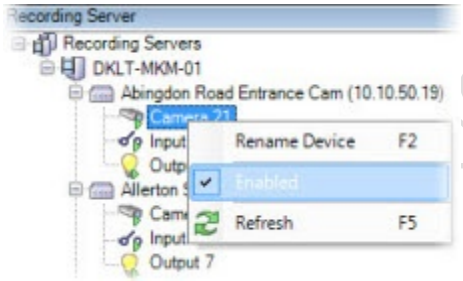
Se puede ver si los dispositivos están activados o desactivados (los ejemplos muestran una salida):

Inhabilitado
Habilitado

El mismo método de activación / desactivación se utiliza para las cámaras, micrófonos, altavoces, metadatos, entradas y salidas.

1. Ampliar el servidor de grabación y el dispositivo. Haga clic en el dispositivo que desee habilitar.

2. Seleccione **Habilitado** para borrar o seleccionarla.



Configurar una conexión segura con el hardware

Puede configurar una conexión HTTPS segura mediante SSL (Secure Sockets Layer) entre el hardware y el servidor de grabación.

Consulte a su proveedor de cámaras para obtener un certificado para su hardware y cargarlo en el hardware, antes de continuar con los pasos siguientes:

1. En el panel **general**, haga clic en el servidor de grabación y seleccionar el hardware.

2. En la ficha **Configuración**, activar HTTPS. Esto no está activado por defecto.

3. Introduzca el puerto del servidor de grabación a la que está conectada la conexión HTTPS. El número de puerto debe coincidir con el puerto configurado en la página principal del dispositivo.

4. Hacer los cambios necesarios y guardar.

Mover hardware

Hardware móvil (explicado)

Se puede mover de hardware entre la grabación de los servidores que pertenecen al mismo sitio. Después de un movimiento, el hardware y sus dispositivos se ejecutan en el nuevo servidor de grabación y nuevas grabaciones se almacenan en este servidor. La medida es transparente para los usuarios del cliente.

Las grabaciones en el servidor de grabación de edad permanecen allí hasta:

- El sistema los borra cuando expira el tiempo de retención. Las grabaciones que alguien ha protegido con Bloqueo de evidencia (ver "Bloqueo de evidencia (explicado)" en la página 267) no se eliminan hasta que expire el tiempo de retención del bloqueo de pruebas. Se define el tiempo de retención de bloqueo de evidencia cuando se los crea. Potencialmente, el tiempo de retención nunca caduca.

- Que los elimine del nuevo servidor de grabación de cada dispositivo en la pestaña **Registro**.

Si intenta quitar un servidor de grabación que aún contiene grabaciones, recibirá una advertencia.

Si se muda de hardware a un servidor de grabación que actualmente no tiene hardware agregado a ella, los usuarios de los clientes deben cerrar la sesión y para recibir datos desde los dispositivos.

Puede utilizar la función de movimiento de hardware para:

- **Saldo de la carga**: Si, por ejemplo, el disco en un servidor de grabación está sobrecargado, se puede añadir un nuevo servidor de grabación y mover algunos de su hardware.

- **Actualizar**: Si, por ejemplo, tiene que reemplazar el servidor que aloja el servidor de grabación con un modelo más nuevo, puede instalar un nuevo servidor de grabación y mueva el hardware del servidor antiguo al nuevo servidor.

- **Sustituya un servidor de grabación defectuoso**: Si, por ejemplo, el servidor está fuera de línea y nunca se situará en línea, puede mover el hardware para otros servidores de grabación y por lo tanto mantener el sistema en funcionamiento. No se puede acceder a las viejas grabaciones. Ver también reemplazar un servidor de grabación (en la página 460).

Grabaciones remotas

Cuando se mueve el hardware a otro servidor de grabación, el sistema cancela recuperaciones en curso o programadas desde sitios interconectados o almacenamientos de borde en las cámaras. Las grabaciones no se eliminan, pero los datos no se recuperan y se guardan en las bases de datos como se esperaba. Recibe un aviso si este es el caso. Para el usuario XProtect Smart Client, que ha iniciado una recuperación al iniciar mover el hardware, la recuperación de falla. El usuario XProtect Smart Client es notificado y puede volver a intentarlo más tarde.

Si alguien ha movido hardware en un sitio remoto, debe sincronizar manualmente el sitio central con la opción **Actualizar hardware** para reflejar la nueva configuración del sitio remoto. Si no se sincronizan, las cámaras que se han movido permanecen desconectados en el sitio central.

Ver también

Movimiento de hardware (asistente) (en la página 113)

Movimiento de hardware (asistente)

Para mover el hardware de un servidor de grabación a otro, ejecute el asistente **Mover hardware**. El asistente le guiará por los pasos necesarios para completar un movimiento para uno o más dispositivos de hardware.

Requisitos
Antes de iniciar el asistente:

- Asegúrese de que el nuevo servidor de grabación puede acceder a la cámara a través de la red física.
- Instalar el servidor de grabación (ver "Instale el servidor de grabación" en la página 44) que desea mover hardware para.
- Autorizarlo (ver "Autorizar un servidor de grabación" en la página 79) y verificado que es en línea.
- Instale las versiones del mismo paquete de dispositivo (ver "Controladores de dispositivo (explicados)" en la página 462) en el nuevo servidor de grabación que ejecute en el servidor existente.

Para ejecutar el asistente:

1. En el panel de **Navegación del sitio**, seleccione **servidores de grabación**.
2. En el panel **general**, haga clic en el servidor de grabación que desea mover el hardware de o haga clic en un dispositivo de hardware específico.
3. Seleccione **Mover hardware**.

   Si el servidor de grabación que se mueve desde el hardware está desconectado, aparece un mensaje de error. Sólo debe elegir para mover el hardware de un servidor de grabación desconectado si está seguro de que nunca llegará en directo. Si se mueve el hardware de todos modos y el servidor vuelve a estar conectado, se arriesga a un comportamiento inesperado del sistema debido a que tiene el mismo hardware que se ejecuta en dos servidores de grabación para un período. Posibles problemas son, por ejemplo, errores de licencia o eventos que no se envían al servidor de grabación correcto.
4. Si ha iniciado el asistente desde el nivel del servidor de grabación, aparece la página **Seleccione el hardware al que desea mover**. Seleccione los dispositivos de hardware que desea mover.
5. En la página **Seleccione el servidor de grabación que desea mover el hardware para**, seleccione de la lista de servidores de grabación instalado en este sitio.
6. En la página **Seleccione el almacenamiento que quiere usar para grabaciones futuras**, la barra de uso de almacenamiento indica el espacio libre en la base de datos de grabación para las grabaciones en directo, no los archivos. El tiempo de retención total es el periodo de retención para la base de datos de grabaciones y los archivos.
7. El sistema procesa su solicitud.
8. Si el movimiento se realizó correctamente, haga clic en **Cerrar**. Si selecciona el nuevo servidor de grabación en el Management Client, se puede ver el hardware movido y ahora grabaciones se almacenan en este servidor.

   Si el movimiento fracasó, puede solucionar el problema a continuación.

En un sistema interconectado, debe sincronizar manualmente el sitio central en el movimiento de hardware en un sitio remoto para reflejar los cambios en usted, u otro administrador del sistema, hechas en el sitio remoto.

Solución de problemas de hardware Mover

Si un movimiento no tuvo éxito, una de las siguientes razones puede ser la causa:

Tipo de error	Solución de problemas
El servidor de impresión no está conectado o en modo failover.	Asegúrese de que el servidor de grabación no está en línea. Es posible que deba autorizarlo. Si el servidor se encuentra en modo failover, espera y vuelve a intentarlo.
La grabación Servidor es no la último versión.	Actualizar el servidor de grabación para que se ejecute la misma versión que el servidor de gestión.
El servidor de grabación no se pudo encontrar en la configuración.	Asegúrese de que usted ha autorizado el servidor de grabación o que no se ha eliminado.
Actualizar la configuración o la comunicación con el Falló la base de datos de configuración.	Asegúrese de que el servidor SQL está conectado y funcionando.
Detener el hardware en el servidor de grabación actual fallido	Tal vez otro proceso ha bloqueado el servidor de grabación o el servidor de grabación está en modo de error. Asegúrese de que el servidor está realizando la grabación y vuelve a intentarlo.
El hardware no existe.	Asegúrese de que el hardware que intenta mover al mismo tiempo no se ha eliminado del sistema por otro usuario. El escenario es bastante improbable.
El servidor de grabación que el hardware ha sido movido de nuevo en línea es, pero prefirió ignorarlo cuando estaba fuera de línea.	Lo más probable es que haya aceptado que el servidor de grabación viejo no termina de estar en línea de nuevo cuando se inició el asistente **Mover hardware**, pero durante el movimiento, el servidor de vino en línea. Comenzar de nuevo el asistente y seleccione **No** cuando se le pide que confirme si el servidor vuelva a conectarse.

Tipo de error	Solución de problemas
El almacenamiento de grabación fuente no está disponible.	Está intentando mover hardware con dispositivos configurados con un almacenamiento de grabación que actualmente no está conectado. Un almacenamiento de grabación está fuera de línea si el disco está fuera de línea o no está disponible. Asegúrese de que el almacenamiento de la grabación esté en línea y vuelva a intentarlo.
Todos los almacenes de grabación en el servidor de grabación de destino deben estar disponibles.	Está intentando mover el hardware a un servidor de grabación donde uno o más almacenamientos de grabación están actualmente fuera de línea. Asegúrese de que todos los almacenes de grabación en el servidor de grabación de destino estén en línea. Un almacenamiento de grabación está fuera de línea o el disco está fuera de línea o no está disponible.

Gestionar hardware

Info tab (hardware)

Para obtener información acerca de la pestaña **Información** para los servidores remotos, consulte ficha Información (servidor remoto) (ver "Pestaña Información (servidor remoto)" en la página 118).

Pestaña de información (hardware)

Nombre	Descripción
Nombre	Ingresa un nombre. El sistema utiliza el nombre cada vez que el hardware está listado en el sistema y en los clientes. El nombre no tiene que ser único. Al cambiar el nombre del hardware, el nombre se cambia a nivel mundial en el Management Client.
Descripción	Introduzca una descripción del hardware (opcional). La descripción aparece en un número de máquinas en el sistema. Por ejemplo, al mover el puntero del mouse sobre el nombre del hardware en el panel **Vista general** : 
Modelo	Identifica el modelo de hardware.

Nombre	Descripción
Versión	Muestra la versión del firmware del sistema según lo especificado por el fabricante.
Número de serie	Número de serie del hardware según lo especificado por el fabricante. El número de serie es a menudo, pero no siempre, idéntica a la dirección MAC.
Driver	Identifica el controlador que maneja la conexión con el hardware.
ES DECIR	Abre la página de inicio por defecto del proveedor de hardware. Puede utilizar esta página para la administración del hardware.
Dirección	El nombre de host o la dirección IP del hardware.
Dirección MAC	Especifica la dirección de control de acceso al medio (MAC) del hardware del sistema. Una dirección MAC es un número hexadecimal de 12 caracteres que identifica de forma única cada pieza de hardware en una red.

Pestaña Configuración (hardware)

En la ficha **Configuración**, se puede verificar o editar los ajustes para el hardware.

El contenido de la ficha **Configuración** está determinado por el hardware seleccionado y varía en función del tipo de hardware. Para algunos tipos de hardware, la ficha **Configuración** no muestra ningún contenido en absoluto o sólo lectura de contenido.

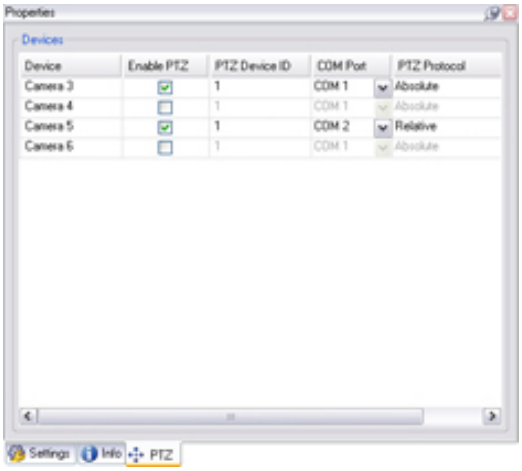
Para obtener información acerca de la pestaña **Configuración** de servidores remotos, ir a la pestaña Configuración (servidor remoto) (en la página 118).

Pestaña PTZ (codificadores de vídeo)

En la pestaña **PTZ**, puede activar PTZ (zoom panorámico) para codificadores de vídeo. La ficha está disponible si el dispositivo seleccionado es un codificador de vídeo o si el controlador es compatible tanto no PTZ y cámaras PTZ.

Debe habilitar el uso de PTZ por separado para cada uno de los canales del codificador de vídeo en la pestaña **PTZ** antes de poder utilizar las funciones PTZ de las cámaras PTZ conectados al codificador de vídeo.

No todos los codificadores de vídeo compatibles con el uso de cámaras PTZ. Incluso los codificadores de vídeo que apoyan el uso de cámaras PTZ pueden requerir una configuración antes de poder utilizar las cámaras PTZ. Por lo general es la instalación de controladores adicionales a través de una interfaz de configuración basada en navegador en la dirección IP del dispositivo.



Pestaña **PTZ**, con PTZ habilitado dos canales en un codificador de vídeo.

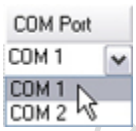
Activar PTZ en un codificador de vídeo

Para habilitar el uso de cámaras PTZ en un codificador de vídeo, haga lo siguiente en la pestaña **PTZ**:

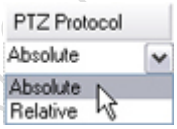
1. En la lista de dispositivos conectados al codificador de vídeo, seleccione la opción **Activar PTZ** cuadro para las cámaras pertinentes:

2. En la columna de la **PTZ ID de dispositivo**, verificar el ID de cada cámara.

3. En la columna de **Puerto COM**, seleccionar qué vídeo del codificador (comunicaciones serie) puertos COM que se utilizará para el control de la funcionalidad PTZ:



4. En la columna de la **Protocolo PTZ**, seleccionar el esquema de posicionamiento que desea utilizar:



   - **Absoluto:** Cuando los operarios se utilizan controles PTZ para la cámara, la cámara está ajustada en relación con una posición fija, a menudo referida como la posición inicial de la cámara
   - **Relativo:** Cuando los operarios se utilizan controles PTZ para la cámara, la cámara se ajusta en relación a su posición actual

   El contenido de la **PTZ protocolo** columna varía mucho dependiendo del hardware. Algunos tienen 5 a 8 protocolos diferentes. Véase también la documentación de la cámara.

5. En la barra de herramientas, haga clic en **Guardar**.

Ya está listo para configurar posiciones predefinidas y patrullaje para cada cámara PTZ:

- Añadir una posición preestablecida (tipo 1) (en la página 149)
- Añadir un perfil de patrullaje (en la página 156)

Administrar servidores remotos

Pestaña Información (servidor remoto)

Nombre	Descripción
Nombre	El sistema utiliza el nombre cada vez que el servidor remoto aparece en el sistema y clientes. El nombre no tiene que ser único. Al cambiar el nombre de un servidor, el nombre se cambia a nivel mundial en el Management Client.
Descripción	Introduzca una descripción del servidor remoto (opcional). La descripción aparece en un número de máquinas en el sistema. Por ejemplo, cuando situando el puntero del ratón sobre el nombre del hardware en el panel **general**.
Modelo	Muestra el producto XProtect instalado en el sitio remoto.
Versión	Muestra la versión del sistema remoto.
Código de licencia de software	El código de licencia de software del sistema remoto.
Driver	Identifica el controlador que maneja la conexión con el servidor remoto.
Dirección	El nombre de host o la dirección IP del hardware.
ES DECIR	(Sólo se aplica al hardware habilitado para Milestone Arcus™) Abre la página de inicio por defecto del proveedor de hardware. Puede utilizar esta página para la administración del hardware o del sistema.
Identificación de sistema remoto	El sistema único de identificación del sitio remoto utilizado por XProtect para, por ejemplo, administrar las licencias.
Nombre de usuario de Windows	Introduzca el nombre de usuario de Windows para el acceso a través del escritorio remoto. No se aplica al hardware habilitado para Milestone Arcus.
Contraseña de windows	Introduzca la contraseña de Windows para el acceso a través del escritorio remoto. No se aplica al hardware habilitado para Milestone Arcus.
Conectar	Abre una conexión remota con el sitio remoto (si se aprueban las credenciales de Windows). No se aplica al hardware habilitado para Milestone Arcus.

Pestaña Configuración (servidor remoto)

En la ficha **Configuración**, puede ver el nombre del sistema remoto.

Pestaña de eventos (servidor remoto)

Puede añadir eventos desde el sistema remoto al sitio central con el fin de crear reglas y con ello responder inmediatamente a los eventos del sistema remoto. El número de eventos dependen de los eventos configurados en el sistema remoto. No se puede eliminar eventos predeterminados.

Si la lista parece ser incompleta:

1. Haga clic con el servidor remoto relevante en el panel **general** y seleccione **Actualizar hardware**.
2. Las listas de los cuadros de diálogo de todos los cambios (dispositivos retirados, actualizan y se añaden) en el sistema remoto desde que se actualizó por última vez establecida o la configuración de Milestone Interconnect. Haga clic en **Confirmar** para actualizar su sitio central con estos cambios.

Pestaña Recuperación remota

En la pestaña **Remoto recuperación**, se puede controlar la configuración de recuperación de la grabación a distancia para el sitio remoto en una configuración de Milestone Interconnect:

Especificar las siguientes propiedades:

Nombre	Descripción
Recuperar grabaciones en Max	Determina el máximo ancho de banda en Kbits / s para ser utilizado para la recuperación de grabaciones de un sitio remoto. Seleccione la casilla de verificación para activar las recuperaciones limitantes.
Recuperar grabaciones entre	Determina que la recuperación de las grabaciones desde un sitio remoto se limitan a un intervalo de tiempo específico. Trabajos sin terminar al final del tiempo continúan hasta la finalización, por lo que si el tiempo final es crítica, es necesario configurar más temprano para permitir trabajos sin terminar para completar. Si el sistema recibe una recuperación automática o solicitud de recuperación desde el XProtect Smart Client fuera del intervalo de tiempo, se acepta, pero no comenzó hasta que se alcanza el intervalo de tiempo seleccionado. Puede ver las tareas pendientes de recuperación de grabación remota iniciadas por los usuarios del **Panel de sistema** -> **Tareas actuales**.
Recuperar en los dispositivos en paralelo	Determina el número máximo de dispositivos desde los que las grabaciones se recuperan de forma simultánea. Cambiar el valor por defecto si necesita más o menos capacidad en función de sus capacidades del sistema.

Cuando se cambia la configuración, pueden pasar varios minutos hasta que los cambios se reflejan en el sistema.

Nada de lo anterior se aplica a la reproducción directa de grabaciones remotas.
Todas las cámaras configuradas como pueden reproducir directamente está disponible para la reproducción directa y ancho de banda usado cuando sea necesario.

Dispositivos

Los dispositivos aparecen en el Management Client cuando se agrega hardware con el asistente **Añadir hardware**.

Puede administrar dispositivos a través de los grupos de dispositivos si tienen las mismas propiedades, consulte Grupos de dispositivos (explicados) (en la página 120).

También puede administrar los dispositivos de forma individual:

- Cámaras
- Micrófonos
- Altavoces
- Metadatos
- Entradas
- Outputs (Salidas)

Ver Dispositivos (explicado) (ver "Dispositivos (explicados)" en la página 123).

Trabajar con grupos de dispositivos

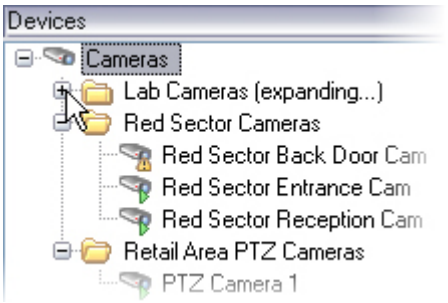
Grupos de dispositivos (explicados)

Agrupación de dispositivos en grupos de dispositivos es parte de la asistente **Añadir hardware**, pero siempre se puede modificar los grupos y añadir más grupos si es necesario.

Usted puede beneficiarse de la agrupación de diferentes tipos de dispositivos (cámaras, micrófonos, altavoces, metadatos, entradas y salidas) en su sistema:

- Los grupos de dispositivos ayudan a mantener una visión general intuitiva de dispositivos en el sistema.
- Los dispositivos pueden existir en varios grupos.
- Puede crear subgrupos y subgrupos en los subgrupos.
- Puede especificar las propiedades comunes para todos los dispositivos dentro de un grupo de dispositivos de una sola vez.
- Propiedades de los dispositivos establecidos a través del grupo no se almacenan para el grupo, pero en los dispositivos individuales.
- Cuando se trata de cometidos, puede especificar la configuración de seguridad comunes para todos los dispositivos dentro de un grupo de dispositivos de una sola vez.
- Cuando se trata de reglas, se puede aplicar una regla para todos los dispositivos dentro de un grupo de dispositivos de una sola vez.

Puede añadir tantos grupos de dispositivos como sea necesario, pero no se pueden mezclar diferentes tipos de dispositivos (por ejemplo, cámaras y altavoces) en un grupo de dispositivos.



Crear grupos de dispositivos con **menos** que 400 dispositivos para que pueda ver y editar todas las propiedades.

Si se elimina un grupo de dispositivos, sólo se elimina el grupo propio dispositivo. Si desea eliminar un dispositivo, por ejemplo una cámara, de su sistema, hacerlo en el nivel de servidor de grabación.

Los siguientes ejemplos se basan en la agrupación de cámaras en grupos de dispositivos, pero los principios se aplican para todos los dispositivos:

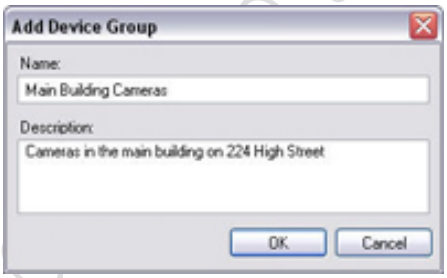
Añadir un grupo de dispositivos (en la página 121)

Especificar los dispositivos a incluir en un grupo de dispositivos (en la página 121)

Epecificar las propiedades comunes para todos los dispositivos en un grupo de dispositivos (en la página 122)

Añadir un grupo de dispositivos

1. En el panel **general**, haga clic en el tipo de dispositivo con el que desea crear un grupo de dispositivos.
2. Seleccione **Añadir grupo de dispositivos**.
3. En el cuadro de diálogo Añadir dispositivo **Grupo**, especificar un nombre y una descripción del nuevo grupo de dispositivos:



La descripción aparece cuando se pasa el puntero del ratón sobre el grupo de dispositivos en la lista del grupo de dispositivos.

4. Haga clic en **OK**. Una carpeta que representa el nuevo grupo de dispositivos aparece en la lista.
5. Continuar con especificar los dispositivos a incluir en un grupo de dispositivos (en la página 121).

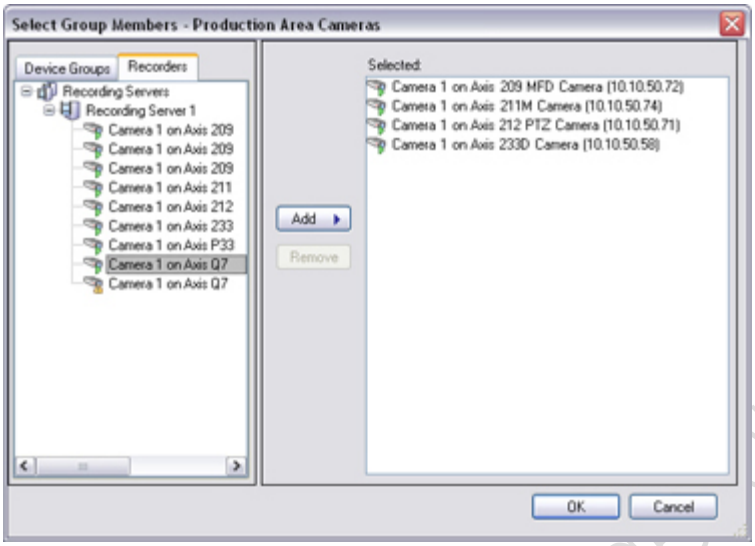
Especificar los dispositivos a incluir en un grupo de dispositivos

1. En el panel **general**, haga clic en la carpeta correspondiente grupo de dispositivos.
2. Seleccione **Editar miembros de grupo de dispositivos**.

3. En la ventana **Seleccionar miembros de grupo**, seleccione una de las pestañas para localizar el dispositivo.

   Un dispositivo puede ser un miembro de más de un grupo de dispositivos.

4. Seleccione los dispositivos que desee incluir y haga clic en **Añadir** o haga doble clic en el dispositivo:



5. Haga clic en **OK** (aceptar).

6. Si supera el límite de 400 dispositivos en un grupo, puede añadir grupos de dispositivos como subgrupos menores de otros grupos de dispositivos:

Epecificar las propiedades comunes para todos los dispositivos en un grupo de dispositivos

Con grupos de dispositivos, puede especificar las propiedades comunes para todos los dispositivos dentro de un grupo determinado dispositivo:

1. En el panel **general**, haga clic en el grupo de dispositivos.

   En el panel **Propiedades**, todas las propiedades **cuales están disponibles en todos los dispositivos del grupo de dispositivos** se enumeran y se agrupan en pestañas.

2. Especificar las propiedades comunes pertinentes.

   En la ficha **Configuración**, puede cambiar entre configuraciones para **todos** dispositivos y configuración de los dispositivos individuales.

3. En la barra de herramientas, haga clic en **Guardar**. Los ajustes se guardan en los dispositivos individuales, no en el grupo de dispositivos.

Trabajar con dispositivos

Dispositivos (explicados)

Hardware tiene una serie de dispositivos que se pueden administrar de forma individual, por ejemplo:

- Una cámara física tiene dispositivos que representan las partes de la cámara (lentes), así como micrófonos, altavoces, metadatos, entrada y salida, ya sea unido o incorporado.
- Un codificador de vídeo tiene varias cámaras analógicas conectadas que aparecen en una lista de dispositivos que representan la parte de la cámara (lentes), así como micrófonos, altavoces, metadatos, entrada y salida, ya sea unido o incorporado.
- Un módulo I / O tiene dispositivos que representan los canales de entrada y de salida para, por ejemplo, luces.
- Un módulo de audio dedicado tiene dispositivos que representan los micrófonos y entradas y salidas de los altavoces.
- En una configuración de Milestone Interconnect, el sistema remoto aparece como hardware con todos los dispositivos del sistema remoto aparece en una lista.

El sistema añade automáticamente los dispositivos del hardware cuando se agrega hardware.

Para obtener información sobre el hardware compatible, consulte la página hardware soportado en el sitio web de Milestone. (https://www.milestonesys.com/supported-hardware)

Las siguientes secciones describen cada uno de los tipos de dispositivos con enlaces a las fichas que puede utilizar para gestionarlos.

Dispositivos de cámara (explicado)

Dispositivos de la cámara se añaden automáticamente al añadir hardware para el sistema y está habilitado de forma predeterminada.

Dispositivos de cámara entregan flujos de vídeo al sistema que los usuarios pueden utilizar el cliente para ver el video en vivo o que el sistema puede grabar para su posterior reproducción por los usuarios del cliente. Los cometidos determinan el derecho de los usuarios a ver el video.

Para obtener información sobre el hardware compatible, consulte la página hardware soportado en el sitio web de Milestone. (https://www.milestonesys.com/supported-hardware)

El sistema viene con una regla de alimentación de inicio predeterminada que asegura que los canales de vídeo de todas las cámaras conectadas se alimentan automáticamente al sistema. Al igual que otras normas, la regla por defecto se puede desactivar y / o modificarse según sea necesario.

Habilitar / deshabilitar y cambiar el nombre de los dispositivos individuales se llevan a cabo en el hardware de servidor de grabación. Ver Activar / desactivar dispositivos a través de grupos de dispositivos (en la página 128).

Para cualquier otra configuración y gestión de cámaras, expanda **Dispositivos** en el panel de navegación del sitio y, a continuación, seleccione **Cámaras**. En el panel Descripción general, que agrupe sus cámaras para una fácil visión general de sus cámaras. La agrupación inicial, se realiza como parte del asistente **Añadir hardware**.

Siga este orden de configuración para completar las tareas más típicas relacionados con la configuración de un dispositivo de cámara:

1. Configurar ajustes de la cámara (véase la ficha Configuración (ver "Pestaña Configuración (dispositivos)" en la página 131)).

2. Configurar transmisiones (ver pestaña Flujos (ver "Pestaña flujos (dispositivos)" en la página 133)).
3. Configurar el movimiento (ver ficha Movimiento (ver "Pestaña de movimiento (dispositivos)" en la página 141)).
4. Configurar la grabación (ver pestaña Registro (ver "Pestaña de grabación (dispositivos)" en la página 135)).
5. Configurar los ajustes restantes, según sea necesario.

Dispositivos de micrófono (explicado)

En muchos dispositivos, puede conectar micrófonos externos. Algunos dispositivos han incorporado en los micrófonos.

Dispositivos de micrófono se añaden automáticamente cuando se agrega hardware al sistema. Están por defecto deshabilitados, por lo que debe habilitarlos antes de su uso, ya sea como parte del asistente **Añadir hardware** o después. Los micrófonos no necesitan licencias por separado. Puede utilizar tantos micrófonos como se requiere en el sistema.

Puede utilizar micrófonos con total independencia de las cámaras.

Dispositivos de micrófono entregan flujos de audio al sistema que los usuarios del cliente pueden escuchar en vivo o el sistema puede grabar para su posterior reproducción por los usuarios del cliente. Puede configurar el sistema para recibir eventos específicos de micrófono que desencadenan acciones pertinentes.

Para obtener información sobre el hardware compatible, consulte la página hardware soportado en el sitio web de Milestone. (https://www.milestonesys.com/supported-hardware)

Los cometidos determinan el derecho de los usuarios a escuchar a los micrófonos. No se puede escuchar a los micrófonos del Management Client.

El sistema viene con un defecto iniciar regla de canal de audio que asegura que el audio se alimenta de todos los micrófonos conectados se alimentan automáticamente al sistema. Al igual que otras normas, la regla por defecto se puede desactivar y / o modificarse según sea necesario.

Habilitar / deshabilitar y cambiar el nombre de los dispositivos individuales se llevan a cabo en el hardware de servidor de grabación. Ver Activar / desactivar dispositivos a través de grupos de dispositivos (en la página 128).

Para cualquier otra configuración y gestión de cámaras, expanda **Dispositivos** en el panel de navegación del sitio y, a continuación, seleccione **Micrófonos**. En el panel Descripción general, que agrupa los micrófonos para una visión general fácil. La agrupación inicial, se realiza como parte de la asistente **Añadir hardware**.

Puede configurar los dispositivos de micrófono en estas pestañas:

- Pestaña Info (ver "Pestaña Información (dispositivos)" en la página 130)
- Pestaña Ajustes (ver "Pestaña Configuración (dispositivos)" en la página 131)
- Pestaña de grabación (ver "Pestaña de grabación (dispositivos)" en la página 135)
- Pestaña de eventos (ver "Pestaña de eventos (dispositivos)" en la página 160)

Dispositivos de altavoces (explicados)

En muchos dispositivos se pueden conectar altavoces externos. Algunos dispositivos han incorporado en los altavoces.

Dispositivos de altavoz se añaden automáticamente cuando se agrega hardware al sistema. Están por defecto deshabilitados, por lo que debe habilitarlos antes de su uso, ya sea como parte del asistente **Añadir hardware**

o después. Altavoces no requieren licencias separadas. Puede utilizar tantos altavoces como se requiere en el sistema.

Puede utilizar los altavoces de forma totalmente independiente de las cámaras.

Para obtener información sobre el hardware compatible, consulte la página hardware soportado en el sitio web de Milestone. (https://www.milestonesys.com/supported-hardware)

El sistema envía un flujo de audio a los altavoces cuando un usuario pulsa el botón de hablar en XProtect Smart Client. Audio del altavoz sólo se registra cuando se le habla por un usuario. Los cometidos determinan el derecho de los usuarios a hablar a través de los altavoces. No se puede hablar a través de los altavoces del Management Client.

Si dos usuarios quieren hablar al mismo tiempo, los cometidos determinan el derecho de los usuarios a hablar a través de los altavoces. Como parte de la definición de los cometidos, puede especificar una prioridad de altavoces de muy alto a muy bajo. Si dos usuarios quieren hablar al mismo tiempo, el usuario cuya cometido tiene la prioridad más alta gana la capacidad de hablar. Si dos usuarios con el mismo cometido quieren hablar al mismo tiempo, se aplica el primer llegado primer servido principio.

El sistema viene con un defecto iniciar regla de canal de audio que se inicia el dispositivo para que el dispositivo está listo para enviar audio activado por el usuario a los altavoces. Al igual que otras normas, la regla por defecto se puede desactivar y / o modificarse según sea necesario.

Habilitar / deshabilitar y cambiar el nombre de los dispositivos individuales se llevan a cabo en el hardware de servidor de grabación. Ver Activar / desactivar dispositivos a través de grupos de dispositivos (en la página 128).

Para cualquier otra configuración y gestión de cámaras, expanda **Dispositivos** en el panel de navegación del sitio y, a continuación, seleccione **Altavoces**. En el panel Descripción general, que los grupos de los altavoces para una visión general fácil. La agrupación inicial, se realiza como parte de la asistente **Añadir hardware**.

Puede configurar los dispositivos de altavoz en estas pestañas:

- Pestaña Info (ver "Pestaña Información (dispositivos)" en la página 130)
- Pestaña Ajustes (ver "Pestaña Configuración (dispositivos)" en la página 131)
- Pestaña de grabación (ver "Pestaña de grabación (dispositivos)" en la página 135)

Dispositivos de metadatos (explicados)

Dispositivos de metadatos proporcionan flujos de datos al sistema que los usuarios pueden utilizar el cliente para ver los datos acerca de los datos, por ejemplo, datos que describen la imagen de vídeo, el contenido o los objetos en la imagen, o la ubicación de donde se grabó la imagen. Los metadatos pueden ser conectados a las cámaras, micrófonos o altavoces.

Los metadatos pueden ser generado por:

- El dispositivo en sí la entrega de los datos, por ejemplo la entrega de la cámara de vídeo.
- Un sistema de terceros o integración a través de un controlador de metadatos genérico.

Los metadatos generada por el dispositivo se vincula automáticamente a uno o más dispositivos en el mismo hardware.

Para obtener información sobre el hardware compatible, consulte la página hardware soportado en el sitio web de Milestone. (https://www.milestonesys.com/supported-hardware)

Los cometidos determinan el derecho de los usuarios para acceder a los metadatos.

El sistema viene con una regla de alimentación de inicio por defecto que garantiza que los metadatos se alimentan de todo el hardware conectado que soporta metadatos, se alimenta automáticamente al sistema. Al igual que otras normas, la regla por defecto se puede desactivar y / o modificarse según sea necesario.

Habilitar / deshabilitar y cambiar el nombre de los dispositivos individuales se llevan a cabo en el hardware de servidor de grabación. Ver Activar / desactivar dispositivos a través de grupos de dispositivos (en la página 128).

Para cualquier otra configuración y gestión de dispositivos de metadatos, expanda **Dispositivos** en el panel de navegación del sitio y, a continuación, seleccione **Metadatos**. En el panel Descripción general, agrupar sus dispositivos de metadatos para una visión general fácil. La agrupación inicial, se realiza como parte de la asistente **Añadir hardware**.

Puede configurar los dispositivos de metadatos en estas pestañas:

- Pestaña Info (ver "Pestaña Información (dispositivos)" en la página 130)
- Pestaña Ajustes (ver "Pestaña Configuración (dispositivos)" en la página 131)
- Pestaña de grabación (ver "Pestaña de grabación (dispositivos)" en la página 135)

Dispositivos de entrada (explicados)

En muchos dispositivos, puede conectar unidades externas a los puertos de entrada del dispositivo. Unidades de entrada suelen ser sensores externos. Puede utilizar este tipo de sensores externos, por ejemplo, para detectar si se abren las puertas, ventanas o puertas. De entrada a partir de tales unidades de entrada externos se trata como eventos por el sistema.

Puede utilizar este tipo de eventos en reglas. Por ejemplo, se podría crear una regla que especifica que una cámara debe empezar a grabar cuando se activa una entrada, y detener la grabación 30 segundos después de la entrada está desactivada.

Es posible utilizar dispositivos de entrada de forma totalmente independiente de las cámaras.

Antes de especificar el uso de unidades externas de entrada en un dispositivo, compruebe que el dispositivo en sí reconocen el funcionamiento del sensor. La mayoría de los dispositivos pueden mostrar esto en sus interfaces de configuración, o por medio de Common Gateway Interface (CGI) comandos de script.

Los dispositivos de entrada son añadidos automáticamente al añadir hardware para el sistema. Están por defecto deshabilitados, por lo que debe habilitarlos antes de su uso, ya sea como parte del asistente **Añadir hardware** o después. Los dispositivos de entrada no requieren licencias separadas. Puede utilizar tantos dispositivos de entrada como se requiere en el sistema.

Para obtener información sobre el hardware compatible, consulte la página hardware soportado en el sitio web de Milestone. (https://www.milestonesys.com/supported-hardware)

Habilitar / deshabilitar y cambiar el nombre de los dispositivos individuales se llevan a cabo en el hardware de servidor de grabación. Ver Activar / desactivar dispositivos a través de grupos de dispositivos (en la página 128).

Para cualquier otra configuración y gestión de cámaras, expanda **Dispositivos** en el panel de navegación del sitio y, a continuación, seleccione **Entrada**. En el panel Descripción general, agrupar sus dispositivos de entrada para una visión general fácil. La agrupación inicial, se realiza como parte de la asistente **Añadir hardware**.

Puede configurar los dispositivos de entrada de estas fichas:

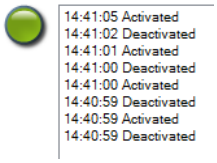
- Pestaña Info (ver "Pestaña Información (dispositivos)" en la página 130)
- Pestaña Ajustes (ver "Pestaña Configuración (dispositivos)" en la página 131)

- Pestaña de eventos (ver "Pestaña de eventos (dispositivos)" en la página 160)

Activar el ingreso de forma manual para la prueba

Con la función de las normas, se definen reglas que se activan de forma automática o desactivar la entrada o puede activar de forma manual y comprobar el resultado en el Management Client:

1. En el panel **general**, seleccionar el dispositivo de entrada correspondiente.
2. Activar la entrada en el dispositivo físico.
3. En el panel **Prever**, compruebe si el indicador se ilumina en verde. A continuación, el dispositivo de entrada funciona.



Dispositivos de salida (explicados)

En muchos dispositivos, puede conectar unidades externas a los puertos de salida del dispositivo. Esto le permite activar / desactivar las luces, sirenas, etc. a través del sistema.

Puede utilizar la salida al crear reglas. Puede crear reglas que activan o desactivan las salidas de forma automática, y las reglas que desencadenan acciones cuando se cambia el estado de una salida.

La salida puede ser activado manualmente desde el Management Client y el XProtect Smart Client.

Antes de especificar el uso de unidades de salida externas en un dispositivo, compruebe que el dispositivo en sí puede controlar el dispositivo conectado a la salida. La mayoría de los dispositivos pueden mostrar esto en sus interfaces de configuración, o por medio de Common Gateway Interface (CGI) comandos de script.

Los dispositivos de salida se añaden automáticamente cuando se agrega hardware al sistema. Están por defecto deshabilitados, por lo que debe habilitarlos antes de su uso, ya sea como parte del asistente **Añadir hardware** o después. Los dispositivos de salida no requieren licencias separadas. Puede utilizar tantos dispositivos de salida como se requiere en el sistema.

Para obtener información sobre el hardware compatible, consulte la página hardware soportado en el sitio web de Milestone. (https://www.milestonesys.com/supported-hardware)

Habilitar / deshabilitar y cambiar el nombre de los dispositivos individuales se llevan a cabo en el hardware de servidor de grabación. Ver Activar / desactivar dispositivos a través de grupos de dispositivos (en la página 128).

Para cualquier otra configuración y administración de cámaras, expanda **Dispositivos** en el panel de navegación del sitio y luego seleccione **Salida**. En el panel Descripción general, agrupar sus dispositivos de entrada para una visión general fácil. La agrupación inicial, se realiza como parte del asistente **Añadir hardware**.

Puede configurar los dispositivos de salida de estas fichas:

- Pestaña Info (ver "Pestaña Información (dispositivos)" en la página 130)
- Pestaña Ajustes (ver "Pestaña Configuración (dispositivos)" en la página 131)

Activar la salida de forma manual para la prueba

Con la función de las normas, se definen reglas que se activan de forma automática o desactivar la salida o se puede activar de forma manual desde un cliente.

Puede activar una salida manualmente desde el Management Client para probar la funcionalidad:

1. En el panel **general** seleccione el dispositivo de salida correspondiente.
2. Por lo general, los siguientes elementos se muestran para cada salida en el panel de **vista previa**:

3. Seleccionar / borrar la casilla de verificación para activar / desactivar la salida seleccionada. Cuando se activa una salida, el indicador se ilumina en verde:

4. También puede hacer clic en el botón rectangular para activar la salida durante la duración definida en la **Tiempo de activación de salida** ajuste en el **Configuración** ficha (es posible que esta función / configuración no esté disponible para todas las salidas). Después de la duración definida, la salida se desactiva automáticamente.

Activar / desactivar dispositivos a través de grupos de dispositivos

Puede activar / desactivar dispositivos sólo a través del hardware configurado. A no ser activado / desactivado en el asistente Añadir hardware de forma manual, dispositivos de cámara son activado por defecto y todos los demás dispositivos son desactivada de forma predeterminada.

Para localizar un dispositivo a través de los grupos de dispositivos para activar o desactivar:

1. En el panel de **Navegación del sitio**, seleccione el dispositivo.
2. En el panel **general** expanda el grupo correspondiente y encontrar el dispositivo.
3. Haga clic en el dispositivo y seleccione **Ir al hardware**.
4. Haga clic en el nodo más para ver todos los dispositivos del hardware.
5. Haga clic en el dispositivo que desea activar / desactivar y seleccione **Activado**.

Los iconos de estado de los dispositivos

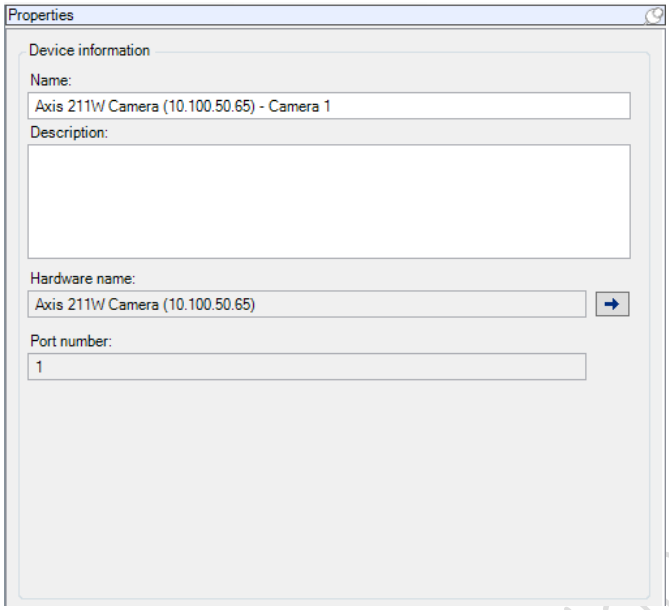
Cuando se selecciona un dispositivo, información sobre el estado actual aparece en el panel de **Prever**. Los siguientes iconos indican el estado de los dispositivos:

Leva-era	Micro-fono	Alta-voz	Meta-datos	En-trada	Salida	Descripción
						**Dispositivo activado y recuperación de datos:** El dispositivo está activado y recuperar una transmisión en vivo.
						**Grabación del dispositivo:** El dispositivo está grabando los datos en el sistema.
						**El dispositivo se detuvo temporalmente o no tiene alimentación:** Cuando se detiene, no hay información se transfiere al sistema. Si se trata de una cámara, no se puede ver vídeo en directo. Un dispositivo parado todavía puede comunicarse con el servidor de grabación para la recuperación de eventos, el establecimiento de la configuración, etc. , a diferencia de cuando un dispositivo está desactivado.
						**Dispositivos desactivados:** No se puede iniciar de forma automática a través de una regla y no puede comunicarse con el servidor de grabación. Si una cámara está desactivada, no se puede ver vídeo en directo o grabado.
						**Base de datos de dispositivo que está siendo reparado.**
						**El dispositivo requiere atención**: El dispositivo no funciona correctamente. Sitúe el puntero del ratón sobre el icono del dispositivo para obtener una descripción del problema en la descripción.
						**Estado desconocido**: Estado del dispositivo se conoce, por ejemplo, si el servidor de grabación no está en línea.
						Tenga en cuenta que algunos iconos se pueden combinar, como en este ejemplo donde **activar dispositivos y recuperación de datos** se combina con la **grabación dispositivo**.

Pestaña Información (dispositivos)

Ficha Información (explicada)

En la ficha **Información**, puede ver y editar información básica acerca de un dispositivo en varios campos. Todos los dispositivos tienen **Información** pestaña.



Propiedades de la pestaña información

Nombre	Descripción
Nombre	El nombre se utiliza cada vez que el dispositivo se incluye en el sistema y clientes. Al cambiar el nombre de un dispositivo, el nombre se cambia a nivel mundial en el Management Client.
Descripción	Introduzca una descripción del dispositivo (opcional). La descripción aparece en un número de máquinas en el sistema. Por ejemplo, cuando se detiene el puntero del ratón sobre el nombre en el panel **general**.
Nombre de hardware	Muestra el nombre del hardware, con la que está conectado el dispositivo. El campo no se edita desde aquí, pero puede cambiarlo haciendo clic en **Ir a** junto a él. Esto le llevará a la información de hardware donde se puede cambiar el nombre.
Número de puerto	Muestra el puerto en el que está conectado el dispositivo en el hardware. Para el hardware de un solo dispositivo, el número de puerto es típicamente **1.** Para el hardware de múltiples dispositivos, tales como servidores de vídeo con varios canales, el número de puerto normalmente indica el canal en el que está conectado el dispositivo, por ejemplo **3.**

Nombre	Descripción
Nombre corto	Para aplicar un nombre corto a la cámara, introdúzcala aquí.La longitud máxima de los caracteres es 128. Si está utilizando plano inteligente, automáticamente el nombre abreviado se muestra con la cámara en el plano inteligente. De lo contrario, se mostrará el nombre completo.
Coordenadas GPS	Introduzca la ubicación geográfica de la cámara en el formato latitud, longitud.El valor introducido determina la posición del icono de la cámara en el plano inteligente en XProtect Smart Client. El campo es principalmente para el plano inteligente y las integraciones de terceros.
Dirección	Introduzca la dirección de visualización de la cámara medida contra un punto norte correcto en un eje vertical.El valor introducido determina la dirección del icono de la cámara en el plano inteligente en XProtect Smart Client. El valor predeterminado es 0,0. El campo es principalmente para el plano inteligente y las integraciones de terceros.
Campo de visión	Introduzca el campo de visión en grados.El valor introducido determina el campo de visión del icono de la cámara en el plano inteligente en XProtect Smart Client. El valor predeterminado es 0,0. El campo es principalmente para el plano inteligente y las integraciones de terceros.
Profundidad	Introduzca la profundidad de la cámara en metros o pies.El valor que ingresa determina la profundidad del icono de la cámara en el plano inteligente en XProtect Smart Client. El valor predeterminado es 0,0. El campo es principalmente para el plano inteligente y las integraciones de terceros.
Vista previa en el navegador	Para verificar que ha introducido las coordenadas GPS correctas, haga clic en el botón.Google Maps se abrirá en su navegador de Internet estándar en la posición que especifique. El campo es principalmente para el plano inteligente y las integraciones de terceros.

Pestaña Configuración (dispositivos)

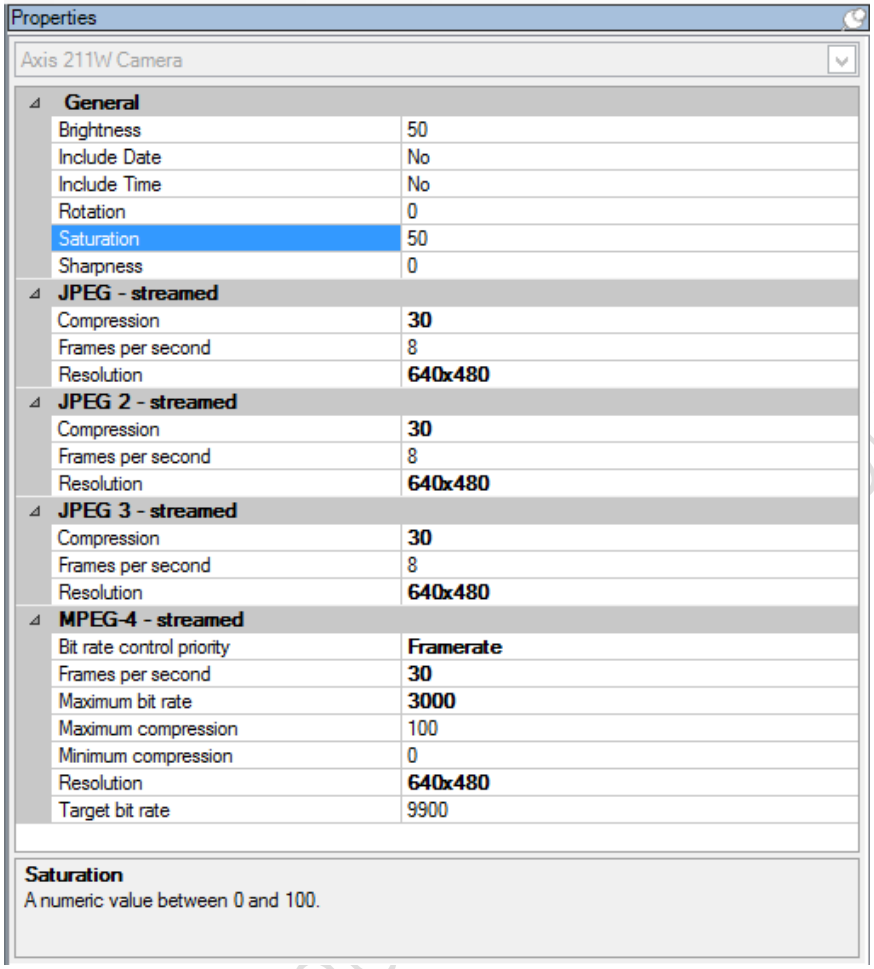
Ficha Configuración (explicada)

En la ficha **Configuración**, puede ver y editar la configuración de un dispositivo en varios campos. Todos los dispositivos **Configuración** pestaña.

Los valores aparecen en una tabla como modificable o de sólo lectura. Cuando cambia una configuración a un valor no predeterminado, el valor aparece **en en negrita**.

El contenido de la tabla depende del controlador de dispositivo.

Rangos permitidos aparecen en el cuadro de información por debajo de la tabla de ajustes:



Configuración de la cámara (explicada)

Puede ver o editar la configuración, tales como:

- velocidad de fotogramas predeterminada
- resolución
- compresión
- El número máximo de fotogramas entre los fotogramas clave
- visualización de la fecha / hora / texto en pantalla de una cámara seleccionada o para todas las cámaras dentro de un grupo de dispositivos.

Los controladores de las cámaras determinan el contenido de la pestaña **Configuración**. Los controladores varían dependiendo del tipo de cámara.

Para cámaras que admiten más de un tipo de flujo, por ejemplo MJPEG y MPEG-4 / H.264 / H.265, puede utilizar multi-streaming, consulte Multi-streaming (explicado) (en la página 134).

Cuando cambia una configuración, puede comprobar rápidamente el efecto de su cambio si tiene el panel **Prever** habilitado. No se puede utilizar el panel de **vista previa** para juzgar el efecto de los cambios de velocidad de cuadro, porque las imágenes en miniatura del **del panel de vista previa** utilizan otro tipo de trama definida en el cuadro de diálogo **Opciones**.

Si cambia la configuración de **máx. fotogramas entre fotogramas clave** y **modo máx. fotogramas entre fotogramas clave**, puede disminuir el rendimiento de algunas funcionalidades en XProtect Smart Client. Por ejemplo, XProtect Smart Client requiere un fotograma clave para poner en marcha visualizar vídeo, por lo que un período más largo entre los fotogramas clave, prolonga el XProtect Smart Client puesta en marcha.

Pestaña flujos (dispositivos)

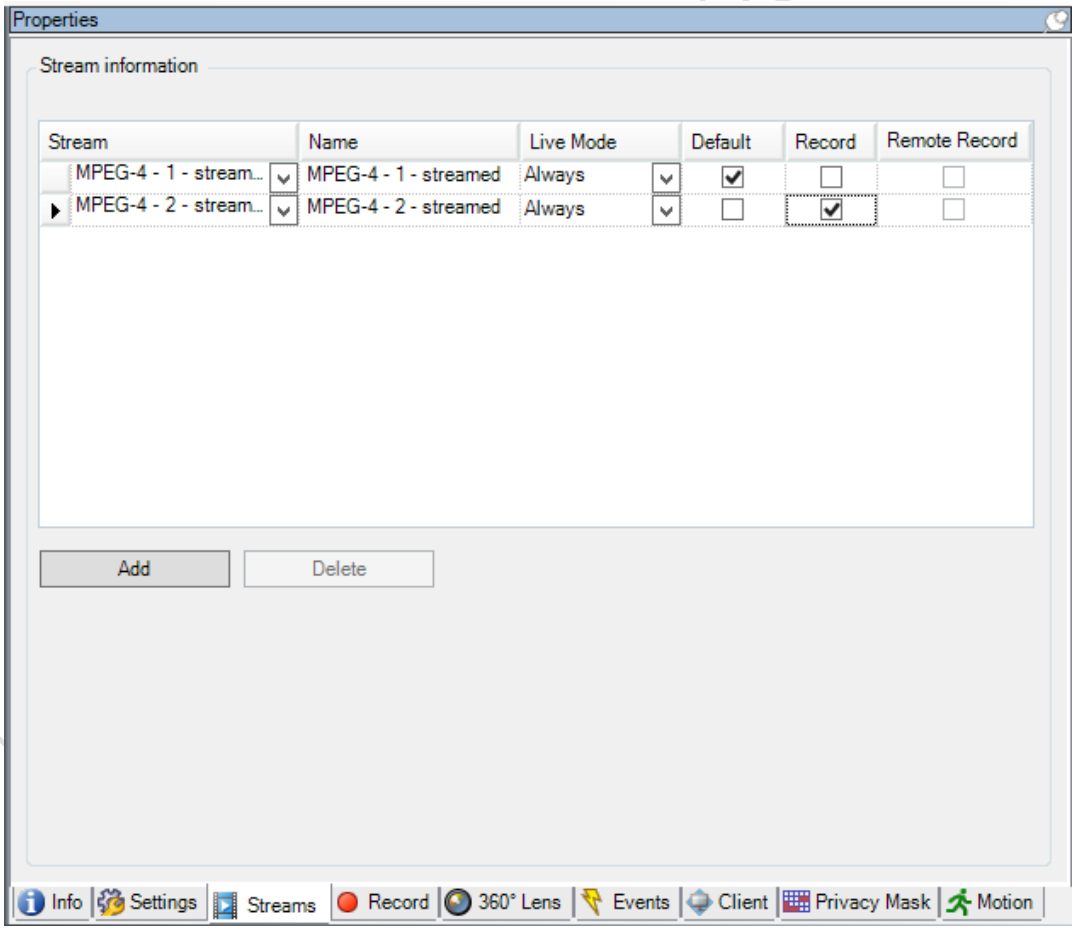
Pestaña Streams (explicada)

Los siguientes dispositivos tienen una pestaña **Flujos**:

- Cámaras

La ficha **Flujos** lista de forma predeterminada una única secuencia. Es corriente por defecto de la cámara seleccionada, que se utiliza para el vídeo en directo y grabado.

Para la transmisión en vivo, se puede configurar y utilizar tantas corrientes viven como soportes de la cámara, pero sólo se puede seleccionar una corriente de grabación a la vez. Para cambiar la secuencia de utilizar para la grabación, seleccione la casilla **Registro** de la corriente que va a grabar.



Multi-streaming (explicado)

La reproducción de vídeo grabado y la visualización de vídeo en directo no requieren necesariamente el mismo tipo de calidad de vídeo y el marco para lograr el mejor resultado. Usted puede tener **cualquiera** una corriente de visualización en directo y otra corriente con fines de reproducción **o** múltiples pistas en directo por separado con diferente resolución, codificación y velocidad de fotogramas.

Ejemplo 1, en vivo y vídeo grabado:

- Para ver el vídeo **en directo**, su organización puede preferir H.264 a una velocidad de fotogramas alta.
- Para la reproducción de **video grabado**, su organización puede preferir MJPEG a una velocidad más baja, porque esto conserva espacio en disco.

Ejemplo 2, varios videos en vivo:

- Para ver vídeo en vivo **desde un punto de funcionamiento local**, su organización puede preferir H.264 a una velocidad de fotogramas alta para tener la más alta calidad de vídeo disponible.
- Para ver **vídeos en directo desde un punto de trabajo conectada a distancia** su organización puede preferir MJPEG a una velocidad más baja y la calidad con el fin de preservar el ancho de banda de red.

Si habilita **Multidifusión en directo** en la ficha **Cliente** de la cámara, sólo funciona en la secuencia de vídeo predeterminada.

Incluso cuando las cámaras de soporte multi-streaming, capacidades de transmisión múltiple individuales pueden variar entre las diferentes cámaras. Consulte la documentación de la cámara para obtener más información.

Para ver si una cámara ofrece diferentes tipos de flujos, consulte pestaña **ajustes**.

Añadir una corriente

1. En la ficha **Flujos**, haga clic en **Añadir**. Esto añade una segunda corriente a la lista.
2. En la columna **Nombre**, edite el nombre de la secuencia. El nombre aparece en XProtect Smart Client.
3. En la columna de la **Modo Directo**, seleccione cuando se necesita la transmisión en vivo.
   - **Siempre**: la corriente funciona aunque no haya usuarios XProtect Smart Client solicitan la corriente.
   - **Nunca**: el flujo está desactivado. Sólo debe utilizarse para los flujos de grabación, por ejemplo, si desea grabaciones en alta calidad y necesita el ancho de banda.
   - **Cuando sea necesario**: la corriente comienza cuando un usuario de solicitudes XProtect Smart Client para ello.
4. En la columna de la **predeterminado**, seleccione la que la corriente es por defecto.
5. En la columna **Grabar**, active la casilla de verificación si desea grabar esta corriente o dejarla desactivada si sólo desea utilizarlo para video en vivo.
6. **Haga clic en Guardar**.

Importante: Si establece una secuencia en **Por defecto** o **Grabar**, la secuencia siempre se ejecuta independientemente de la configuración **Modo Directo**. Selección **Cuando sea necesario** y **siempre** tendrá

el mismo efecto en el sistema y si selecciona **Nunca**, la corriente se está ejecutando, pero no se puede ver en vivo.

Si no desea que las corrientes que se ejecuten en absoluto a menos que alguien está viendo vídeo en directo, se puede modificar la **Regla por defecto de iniciar directo** para iniciar, a petición de la predefinido RSS **vivo cliente solicitó** evento.

Pestaña de grabación (dispositivos)

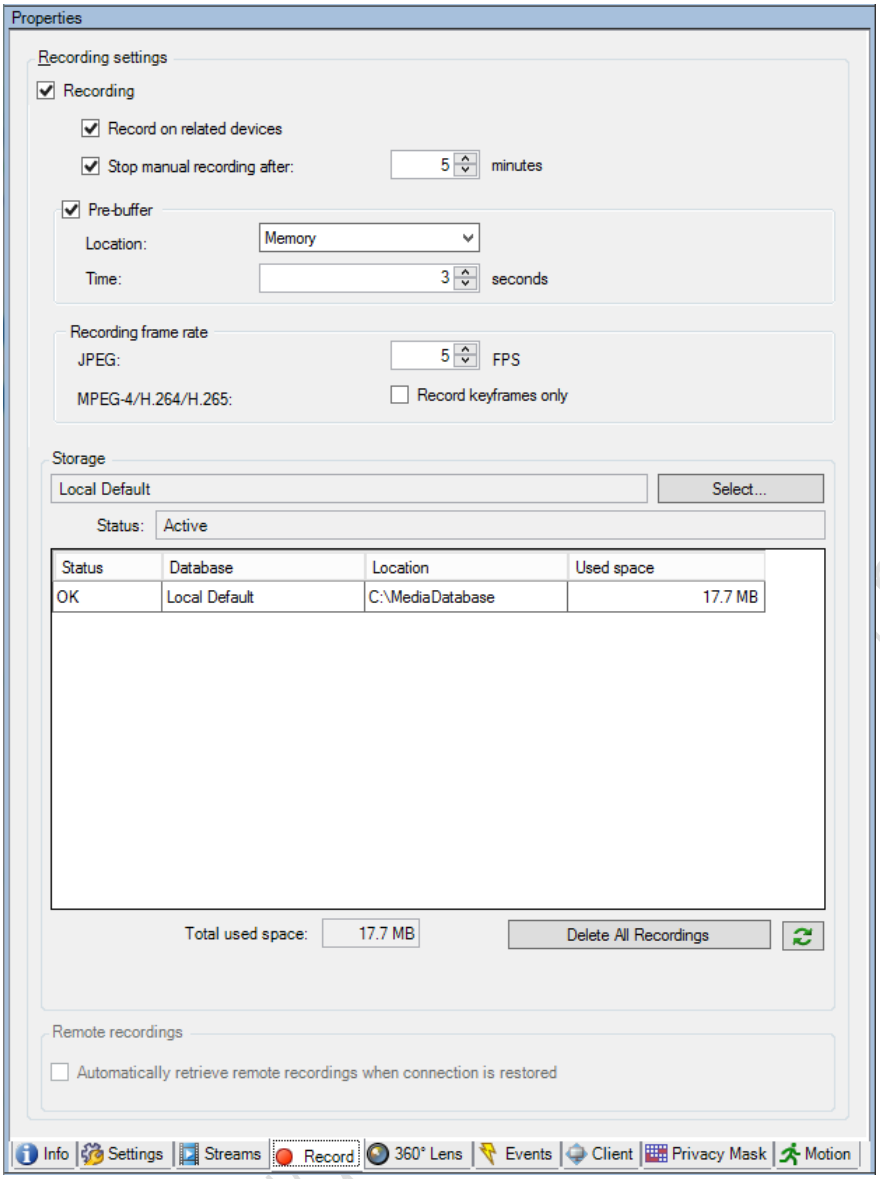
Ficha Registro (explicada)

Los siguientes dispositivos cuentan con una pestaña **Registro**:

- Cámaras
- Micrófonos
- Altavoces
- Metadatos

Las grabaciones de un dispositivo sólo se guardan en la base de datos cuando se ha activado la grabación y se cumplen los criterios de la regla relacionados con la grabación.

Los parámetros que no se pueden configurar para un dispositivo están atenuados.



Activar / desactivar la grabación

La grabación está activada de forma predeterminada. Para activar la grabación / desactivar:

1. En el panel de **Navegación del sitio**, seleccione **servidores de grabación**.
2. Seleccione el dispositivo correspondiente en el panel **general**.
3. En la pestaña **Grabar**, active o desactive la casilla de verificación **grabación**.

Debe habilitar la grabación para el dispositivo antes de poder grabar los datos de la cámara. Una regla que especifica las circunstancias para un dispositivo de registro no funcionará si tiene desactivada la grabación para el dispositivo.

Permitir la grabación en dispositivos relacionados

Para dispositivos de la cámara, se puede activar la grabación de dispositivos relacionados, por ejemplo, micrófonos que están conectados al mismo servidor de grabación. Esto significa que el registro de dispositivos relacionados cuando la cámara graba.

Las grabaciónes en dispositivos relacionados están habilitadas de forma predeterminada para los nuevos dispositivos de la cámara, pero se puede desactivar y activar como desee. Para dispositivos de cámara existente en el sistema, la casilla de verificación está desactivada de forma predeterminada.

1. En el panel de **Navegación del sitio**, seleccione **servidores de grabación**.
2. Seleccione el dispositivo de cámara correspondiente en el panel **general**.
3. En la pestaña **Grabar**, active o desactive caja **Grabar en dispositivos relacionados**.
4. En la ficha de **cliente**, especificar los dispositivos que se relacionan con esta cámara.

Si desea activar la grabación en dispositivos relacionados que están conectados a otro servidor de grabación, debe crear una regla.

Pre-buffering (explicado)

Pre-buffering es la capacidad de grabar audio y vídeo antes de que ocurra el evento de activación real. Esto es útil cuando se desea grabar el audio o el vídeo que conduce a un evento que desencadena la grabación, por ejemplo, la apertura de una puerta.

Pre-buffering es posible debido a que el sistema recibe continuamente los flujos de audio y vídeo desde los dispositivos conectados y los almacena temporalmente en el período pre-búfer intermedio.

- Si se activa una regla de grabación, las grabaciones temporales se hacen permanentes para el tiempo de pre-grabación configurado de la regla.
- Si se activa ninguna regla de grabación, las grabaciones temporales en la pre-buffer se eliminan automáticamente después de que el tiempo de pre-búfer intermedio.

Para utilizar la función de pre-buffer, los dispositivos deben estar habilitadas y el envío de una corriente al sistema.

El almacenamiento de las grabaciones pre-buffer temporal

Se puede elegir la ubicación de almacenamiento de las grabaciones pre-búfer temporal:

- En la memoria; el período pre-buffer se limita a 15 segundos.
- En el disco (en la base de datos de medios); se puede elegir todos los valores.

Almacenamiento en la memoria en lugar de en el disco mejora el rendimiento del sistema, pero sólo es posible para los períodos pre-tampón más cortos.

Cuando las grabaciones se almacenan en la memoria, y se hacen algunas de las grabaciones temporales permanente, las grabaciones temporales restantes se eliminan y no se pueden recuperar. Si tiene que ser capaz de mantener las grabaciones restantes, almacenar las grabaciones en el disco.

Los dispositivos que admiten pre-buffering

Cámaras, micrófonos y altavoces compatibles con pre-buffering. Para los altavoces, los flujos sólo se envían cuando el usuario XProtect Smart Client utiliza la función **Hablar con el altavoz**. Esto significa que dependiendo de cómo sus corrientes de altavoz se activan para ser registrado hay poco o ningún pre-buffering disponible.

En la mayoría de los casos, configura los altavoces para grabar cuando el usuario XProtect Smart Client utiliza la función **Hablar con el altavoz** . En tales casos, no hay ningún altavoz pre-buffer está disponible.

Administrar pre-buffering

Activar y desactivar pre-buffering:

Pre-buffering está activado por defecto con un tamaño de pre-buffer de tres segundos y el almacenamiento de la memoria.

1. Para activar / desactivar la pre-buffering, seleccione / desactivar la casilla de verificación **Pre-buffer**.

Especificar la ubicación de almacenamiento y el período de pre-buffer:

Grabaciones pre-buffer temporal se almacenan en la memoria o en el disco:

1. Para **Ubicación**, seleccione **Memoria** o **Disco** y especifique el número de segundos.

   El número de segundos que especifique debe ser lo suficientemente grande como para dar cabida a sus necesidades en las diversas reglas de grabación que defina.

   Si usted requiere un período de pre-buffer de más 15 segundos, seleccione **disco**.
2. Si cambia la ubicación de **memoria**, el sistema reduce el período de 15 segundos automáticamente.

Utilice pre-buffer en reglas:

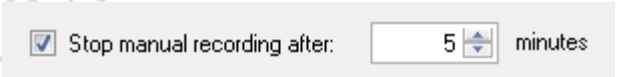
Al crear reglas que desencadenan la grabación, puede seleccionar que las grabaciones deben comenzar algún tiempo antes del evento (pre-buffer).

Ejemplo: La siguiente regla especifica que debe comenzar la grabación de la cámara 5 segundos antes de que se detecte movimiento en la cámara.

Para utilizar la función de grabación de pre-buffer en la norma, debe habilitar pre-buffering en el dispositivo que se está grabando y se debe configurar la longitud pre-buffer a por lo menos la misma longitud que se especifica en la regla.

Manejo de grabación manual

Detener la grabación manual tras está activada de forma predeterminada con un tiempo de grabación de cinco minutos. Esto es para asegurar que el sistema se detiene automáticamente todas las grabaciones iniciadas por los usuarios de XProtect Smart Client.



1. Para activar y desactivar la grabación manual se detenga automáticamente por el sistema, seleccionar / borrar la grabación manual **detener después de casilla de verificación**.
2. Cuando se habilita, especifique un tiempo de grabación. El número de minutos que especifique debe ser lo suficientemente grande como para dar cabida a las necesidades de las diversas grabaciones manuales sin sobrecargar el sistema.

Añadir a los cometidos:

Debe conceder el derecho de iniciar y detener la grabación manual a los usuarios clientes de cada cámara en **Cometidos** en la ficha **Dispositivo**.

El uso en reglas:

Los eventos se pueden utilizar cuando se crea reglas relacionadas con la grabación manual son:

- **Grabación manual iniciada**
- **Grabación manual detenida**

Especificar velocidad de grabación

Se puede especificar la velocidad de grabación para JPEG.

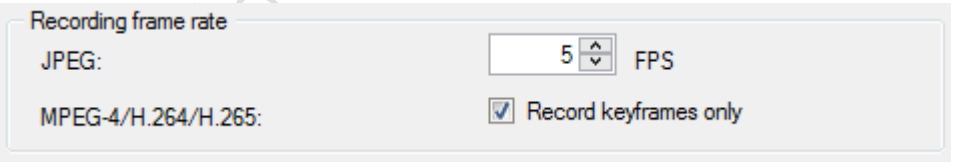
- Seleccione o escriba la frecuencia de fotogramas de grabación (en FPS, fotogramas por segundo) en el **Velocidad de grabación: Caja (JPEG)**.

Permitir la grabación de fotogramas clave

Puede habilitar la grabación fotograma clave para MPEG-4/H.264/H.265 corrientes. Esto significa que el sistema conmuta entre sólo y grabación de todas las tramas en función de la configuración de reglas de fotogramas clave de grabación.

Puede, por ejemplo, dejar que los fotogramas clave de registro del sistema cuando no hay movimiento en la vista y cambiar a todos los marcos sólo en caso de detección de movimiento para ahorrar espacio de almacenamiento.

1. Seleccione los fotogramas clave **registra sólo** caja.

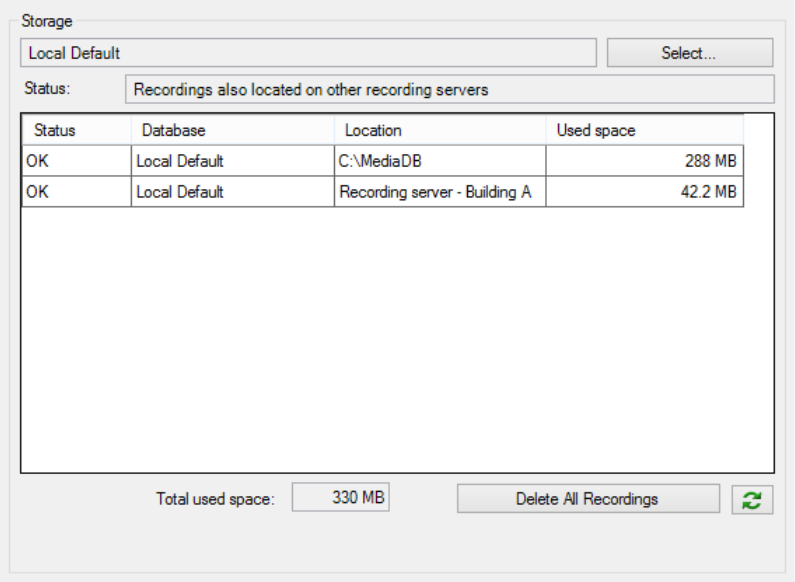


2. Configure una regla que active la función, ver Acciones y acciones de detención (explicadas) (en la página 185).

Almacenamiento (explicado)

Bajo **Almacenamiento**, puede supervisar y gestionar las bases de datos de un dispositivo o un grupo de dispositivos añadidos al mismo servidor de grabación.

Por encima de la mesa, se puede ver la base de datos seleccionada y su estado. En este ejemplo, la base de datos seleccionada es la predeterminada **Valor predeterminado local** y el estado es **Existen grabaciones en otros servidores de grabación.**. El otro servidor es el servidor de grabación en el edificio A.



Los estados posibles de la base de datos seleccionada:

Nombre	Descripción
Existen grabaciones en otros servidores de grabación.	La base de datos está activa y en funcionamiento y tiene grabaciones ubicados en almacenamientos en otros servidores de grabación también.
Los archivos también se encuentran en el almacenamiento anterior	La base de datos está activa y en funcionamiento y tiene archivos ubicados en otros almacenes también.
Activo	La base de datos está activa y en funcionamiento.
Los datos de algunos de los dispositivos seleccionados se están moviendo a otra ubicación	La base de datos está activa y en funcionamiento y el sistema se está moviendo de datos para uno o más seleccionados dispositivos en un grupo de un lugar a otro.
Los datos del dispositivo se están moviendo a otra ubicación en este momento	La base de datos está activa y en funcionamiento y el sistema se está moviendo de datos para el dispositivo seleccionado de un lugar a otro.
Información no disponible en modo de failover	El sistema no puede recoger información de estado sobre la base de datos cuando la base de datos está en modo failover.

Más abajo en la ventana, puede ver el estado de cada base de datos (**OK**, **Desconectado** o **Almacenamiento anterior**), la ubicación de cada base de datos y cuánto espacio utiliza cada base de datos.

Si todos los servidores están en línea, se puede ver el total de espacio utilizado para todo el almacenamiento en el campo **espacio total utilizado**.

Con el botón **Borrar todas las grabaciones**, puede eliminar todas las grabaciones del dispositivo o del grupo de dispositivos si ha agregado todos los dispositivos del grupo al mismo servidor. No se eliminan los datos protegidos.

Para obtener información acerca de la configuración del almacenamiento, consulte almacenamiento y archivo (explicado) (en la página 82).

Grabación remota (explicada)

La opción de grabación a distancia sólo está disponible si la cámara seleccionada es compatible con el almacenamiento borde o es una cámara en una configuración de Milestone Interconnect.

Para asegurarse de que todas las grabaciones se guardan en caso de problemas de red, seleccione **Recuperar automáticamente las grabaciones remotas cuando se restablece la conexión**. Esto permite la recuperación automática de grabaciones una vez que se restablezca la conexión.

El tipo de hardware seleccionado determina dónde se recuperan de grabaciones:

- Para una cámara con almacenamiento local de grabación, las grabaciones se recuperan de almacenamiento local de grabación de la cámara.
- Para un sistema remoto Milestone Interconnect, las grabaciones son recuperados de servidores de grabación de los sistemas remotos.

Puede utilizar las siguientes funciones con independencia de la recuperación automática:

- La grabación manual.
- La regla **Recuperar y almacenar grabaciones remotas desde <dispositivos>**.
- La regla **Recuperar y almacenar grabaciones remotas entre <hora de inicio y fin> de <dispositivos>**.

Pestaña de movimiento (dispositivos)

Pestaña de movimiento (explicada)

Los siguientes dispositivos cuentan con una pestaña **Movimiento**:

- Cámaras

En la ficha **Movimiento**, puede habilitar y configurar la detección de movimiento para la cámara seleccionada. Configuración de detección de movimiento es un elemento clave en el sistema: Su configuración de detección de movimiento determina cuando el sistema genera eventos de movimiento y por lo general también cuando se graba vídeo.

El tiempo invertido en la búsqueda de la mejor configuración posible la detección de movimiento para cada cámara le ayuda a evitar más adelante, por ejemplo, grabaciones innecesarias. Dependiendo de la ubicación física de la cámara, puede ser una buena idea para probar la configuración de detección de movimiento bajo diferentes condiciones físicas como de día / noche y viento / calma.

Antes de configurar la detección de movimiento para una cámara, Milestone recomienda que haya configurado los ajustes de calidad de imagen de la cámara, por ejemplo resolución, codec de vídeo y ajustes de flujo en la pestaña **Configuración**. Si más adelante cambia los ajustes de calidad de imagen, siempre se debe probar cualquier configuración de detección de movimiento después.

Si ha definido áreas con máscaras de privacidad permanentes en la ficha **Protección de privacidad** (ver "**Pestaña Máscara de privacidad (explicada)**" en la página 164), puede optar por mostrar las máscaras de privacidad en la ficha **Movimiento** seleccionando la casilla **Mostrar máscaras de privacidad** .

Nota: No hay detección de movimiento dentro de áreas cubiertas por máscaras de privacidad permanentes.

Puede configurar todos los parámetros de un grupo de cámaras, pero lo más habitual es establecer la excluye regiones por cámara.

- Activar y desactivar la detección de movimiento (en la página 143)
- Especificar la configuración de detección de movimiento (en la página 143)

Activar y desactivar la detección de movimiento

Se especifica la configuración predeterminada de detección de movimiento para las cámaras en el **Herramientas** > **Opciones** > **General** ficha.

Para activar o desactivar la detección de movimiento después de una cámara:

- Active o desactive la casilla de verificación de pestaña **movimiento Detección de movimiento**.

Importante: Al deshabilitar la detección de movimiento para una cámara, las normas relacionadas con la detección de movimiento para la cámara no funcionan.

Especificar la configuración de detección de movimiento

Puede especificar la configuración relacionada con la cantidad de cambios que se requieren en la visión de la cámara para que el cambio que se considere que el movimiento. Por ejemplo, puede especificar intervalos entre el análisis de detección de movimiento y las áreas de una vista en la que se debe ignorar el movimiento. También puede ajustar la precisión de la detección de movimiento y, por tanto, la carga en los recursos del sistema.

Aceleración de hardware (explicada)

Seleccione **Automático** para habilitar la detección de movimiento de video acelerado por hardware. Esta es la configuración predeterminada cuando agrega una cámara. El servidor de grabación ahora usa recursos de GPU si están disponibles. Esto reducirá la carga de la CPU durante el análisis de movimiento de video y mejorará el rendimiento general del servidor de grabación.

La detección de movimiento de video acelerada por hardware usa recursos de GPU en:

- CPU Intel que son compatibles con Intel Quick Sync.
- Adaptadores de pantalla NVIDIA® conectados a su servidor de grabación.

El equilibrio de carga entre los diferentes recursos se realiza automáticamente. En el nodo **Monitor del sistema** , puede verificar si la carga de análisis de movimiento actual en los recursos de la GPU NVIDIA está dentro de los límites especificados desde el nodo **Umbrales del monitor del sistema** . Los indicadores de carga de la GPU NVIDIA son:

- Decodificación de NVIDIA
- Memoria de NVIDIA
- Procesamiento de NVIDIA

Consejo: Si la carga es demasiado alta, puede agregar recursos GPU a su servidor de grabación instalando múltiples adaptadores de pantalla NVIDIA. Milestone no recomienda el uso de la configuración Scalable Link Interface (SLI) de sus adaptadores de pantalla NVIDIA.

Los productos NVIDIA tienen capacidades de cómputo diferentes. Para verificar que su producto NVIDIA sea compatible con la aceleración de hardware para los códecs utilizados en su sistema Milestone XProtect, busque los códecs admitidos para la versión de capacidad informática en la tabla a continuación.

Para conocer la versión de capacidad informática de su producto NVIDIA, visite el sitio web de NVIDIA (https://developer.nvidia.com/cuda-gpus).

Capacidad de cálculo	Arquitectura	H.264	H.265
3.x	Kepler	✓	-
5.x	Maxwell	✓	-

Capacidad de cálculo	Arquitectura	H.264	H.265
6.x	Pascal	✓	✓
7.x	Volta	✓	✓

Para ver si la detección de movimiento de video es hardware acelerado para una cámara específica, habilite el registro en el archivo de registro del servidor de recodificación.Establezca el nivel en **Debug** y los diagnósticos se registran en DeviceHandling.log.El registro sigue el patrón:
[Tiempo] [274] DEBUG - [guid] [nombre] Decodificación configurada:Automático:Decodificación real: Intel / NVIDIA

La versión de sistema operativo del servidor de grabación y la generación de CPU pueden afectar el rendimiento de la detección de movimiento de video acelerado por hardware.La asignación de memoria de la GPU es a menudo el cuello de botella con versiones anteriores (el límite típico es entre 0,5 GB y 1,7 GB).

Los sistemas basados en Windows 10 / Server 2016 y CPU de 6ª generación (Skylake) o más recientes pueden asignar el 50% de la memoria del sistema a GPU y, de este modo, eliminar o reducir este cuello de botella.

CPU de Intel de sexta generación proporciona descodificación acelerada de hardware de H.265, por lo que el rendimiento es comparable con H.264 para estas versiones de CPU.

Sensibilidad dinámica (explicada)

La detección de movimiento es por defecto configurado para sensibilidad dinámica. Para ajustar el nivel de sensibilidad manualmente, ver Habilitar sensibilidad manual (en la página 144).

Milestone recomienda que no habilita la sensibilidad manual, porque:

- Con sensibilidad dinámica, el sistema calcula y optimiza el nivel de sensibilidad de forma automática y suprime las detecciones de movimiento que vienen de ruido en las imágenes.
- Sensibilidad dinámica mejora la detección de movimiento en la noche, donde el ruido en las imágenes a menudo desencadena el movimiento falso.
- El sistema no está sobrecargado por el exceso de grabación.
- Los usuarios no faltan los resultados de demasiado poca grabación.

Habilitar sensibilidad manual

El ajuste de sensibilidad determina **la cantidad cada píxel** en la imagen tiene que cambiar antes de que sea considerado como movimiento.

1. Seleccione la pestaña **Movimiento** casilla de verificación **Sensibilidad manual**.
2. Arrastre el control deslizante hacia la izquierda para un nivel de sensibilidad más alta, ya la derecha para una sensibilidad menor.

   La **mayor** el nivel de sensibilidad, menor será el cambio está permitido en cada píxel antes de que sea considerado como movimiento.

   El **menor** el nivel de sensibilidad, se permite más cambios en cada píxel antes de que sea considerado como movimiento.

   Píxeles en el que se detecta movimiento se resaltan en verde en la imagen de vista previa.

3. Seleccione una posición del botón en la que sólo se resalten las detecciones que usted considere movimiento.

Puede comparar y establecer el ajuste entre las cámaras por el número en la parte derecha de la barra de sensibilidad exacta.

Especificar umbral

El umbral de detección de movimiento determina **el número de píxeles en la imagen** debe cambiar antes de que sea considerado como movimiento.

1. Arrastre el control deslizante hacia la izquierda para un nivel de movimiento superior, y hacia la derecha para un nivel de movimiento inferior.

2. Seleccione una posición del deslizador en el que sólo se detectan las detecciones que considere movimiento.

La línea vertical negro en la barra de indicación de movimiento muestra el umbral de detección de movimiento: Cuando el movimiento es detectado por encima del nivel de umbral de detección seleccionada, la barra cambia de color de verde a rojo, lo que indica una detección positiva.

Movimiento barra de indicación: cambia de color de verde a rojo cuando por encima del umbral, lo que indica una detección de movimiento positivo.

Seleccione Ajustes de fotogramas clave

Determina si la detección de movimiento en los fotogramas clave sólo que en lugar de en toda la secuencia de vídeo. Sólo se aplica a MPEG-4/H.264/H.265.

La detección de movimiento en los fotogramas clave reduce la cantidad de potencia de procesamiento utilizado para llevar a cabo el análisis.

Seleccionar **fotogramas clave única caja (MPEG-4/H.264/H.265)** hacer la detección de movimiento sólo los fotogramas clave.

Intervalo de procesamiento Seleccionar imagen

Se puede seleccionar la frecuencia con el sistema realiza el análisis de detección de movimiento.

A partir de la **proceso imagen cada (ms)** lista:

- Seleccione el intervalo. Por ejemplo, cada 1000 milisegundos son una vez por segundo. El valor por defecto es cada 500 milisegundos.

  El intervalo se aplica si la tasa de fotogramas real es mayor que el intervalo que establezca aquí.

Especificar la resolución de detección

Le permite optimizar el rendimiento de la detección de movimiento mediante el análisis de sólo un porcentaje seleccionado de la imagen, por ejemplo 25%. Mediante el análisis de 25%, sólo cada cuarto píxel de la imagen se analiza en lugar de todos los píxeles.

Usar la detección optimizada reduce la cantidad de potencia de procesamiento utilizado para llevar a cabo el análisis, sino también un medio de detección de movimiento menos precisa.

- En la lista **Resolución de detección**, seleccione la resolución de detección deseada.

Generación de datos de movimiento para la búsqueda inteligente

Con **Generar datos de movimiento para búsqueda inteligente** activada, el sistema genera datos de movimiento para las imágenes utilizadas para la detección de movimiento. Por ejemplo, si selecciona la detección de movimiento en los fotogramas clave única, los datos de movimiento se produce también para sólo los fotogramas clave.

Los datos de movimiento adicional permiten al usuario del cliente, a través de la función de búsqueda avanzada, para buscar rápidamente las grabaciones relevantes basados en movimiento en el área seleccionada de la imagen. El sistema no genera datos de movimiento dentro de las áreas cubiertas por máscaras de privacidad permanentes, sino solo para las áreas con máscaras (ver "Pestaña Máscara de privacidad (explicada)" en la página 164) de privacidad elevables.

Movimiento de umbral de detección y excluir a las regiones no influyen en los datos de movimiento generados.

Se especifica la configuración por defecto de generación de datos de búsqueda avanzadas para las cámaras en las **Herramientas** > **Opciones** > **general** pestaña.

Especificar regiones excluidas

Puede excluir la detección de movimiento de áreas específicas de una vista de cámara.

Nota: Las áreas con máscaras de privacidad permanentes también están excluidas de la detección de movimiento. Seleccione la casilla **Mostrar máscaras de privacidad** para mostrarlas.

Excluir la detección de movimiento de áreas específicas le ayuda a evitar la detección de movimientos irrelevantes, por ejemplo, si la cámara cubre un área donde un árbol se balancea en el viento o donde los autos pasan regularmente en el fondo.

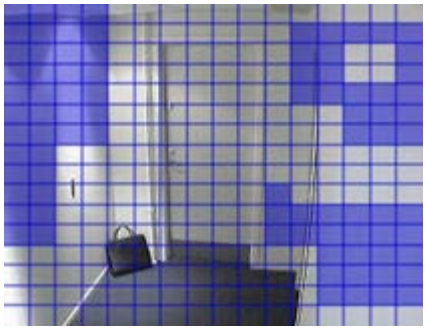
Cuando se utiliza excluir regiones con cámaras PTZ y pan-tilt-zoom de la cámara, el área excluida **no** hace movimiento en consecuencia ya que la zona está cerrada a la imagen de la cámara, y no el objeto.

1. Para utilizar excluir regiones, seleccionar casilla de verificación **Utilizar regiones excluidas**.

   Una cuadrícula divide la imagen de vista previa en secciones seleccionables.

2. Para definir excluir regiones, arrastre el puntero del maous sobre las áreas requeridas en la imagen de vista previa mientras pulsa el botón izquierdo del mouse. El botón derecho del mouse borra una sección de la cuadrícula.

Puede definir tantas regiones excluidas como sea necesario. Las regiones excluidas aparecen en azul:



El azul excluye áreas sólo aparecen en la imagen de vista previa en la ficha **Movimiento**, no en cualquier otra imagen de vista previa en el Management Client de clientes o de acceso.

Pestaña Definiciones (dispositivos)

Pestaña Preajustes (explicada)

Los siguientes dispositivos tienen una pestaña **Preajustes**:

- Las cámaras PTZ que apoyan posiciones preestablecidas

En la ficha **ajustes preestablecidos**, puede crear o posiciones preestablecidas de importación, por ejemplo:

- En reglas para hacer un PTZ (pan-tilt-zoom) mueve la cámara a una posición predeterminada específica cuando se produce un evento.
- En el patrullaje, para el movimiento automático de una cámara PTZ entre un número de posiciones predeterminadas.
- Para la activación manual por los usuarios XProtect Smart Client.

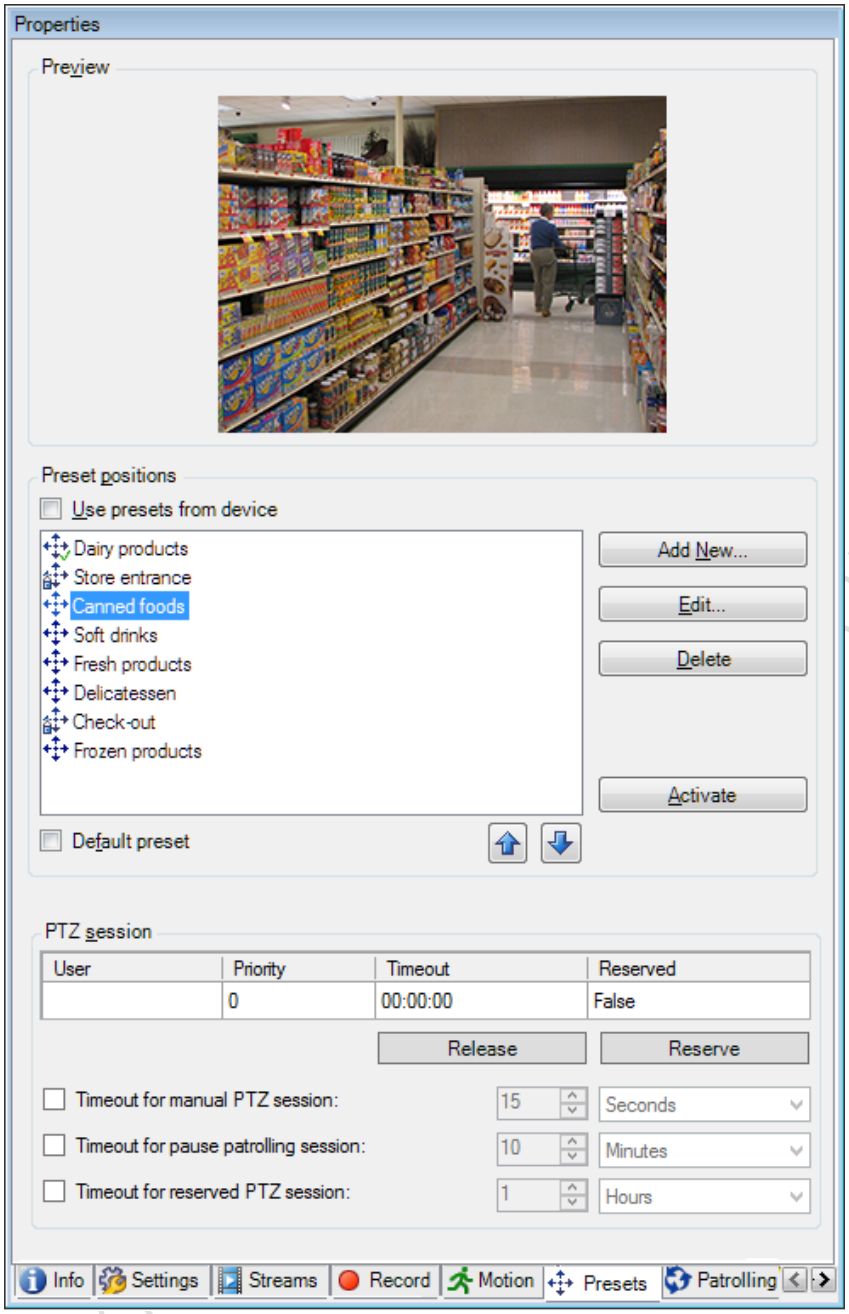
Puede bloquear una posición predeterminada si desea impedir que los usuarios de XProtect Smart Client o usuarios con derechos limitados de seguridad de la actualización de esta preestablecido. Los presets bloqueados se indican con este icono .

Los administradores con derechos de seguridad para ejecutar una sesión reservada PTZ (ver "Sesiones PTZ reservadas (explicación)" en la página 152) puede funcionar la cámara PTZ en este modo. Esto impide que otros usuarios tomar el control de la cámara. Con derechos suficientes, se puede liberar sesiones reservadas PTZ de otros usuarios (ver "Liberar sesión PTZ" en la página 153).

Se asigna el permiso PTZ para cometidos en la ficha Seguridad general (ver "Pestaña de Seguridad General (cometidos)" en la página 234) o en la ficha PTZ (ver "Pestaña PTZ (cometidos)" en la página 256).

Puede controlar si el sistema está patrullando en la actualidad o que un usuario ha tomado el control, en zona **sesión de PTZ** (ver "**Propiedades de sesión PTZ**" en la página 153).

También cambia los tiempos de espera de sesión PTZ para la cámara.



Ajustes preestablecidos de pestañas, con posiciones predeterminadas definidas

Añadir una posición preestablecida (tipo 1) (en la página 149)

Use las posiciones preestablecidas desde el dispositivo (tipo 2) (ver "Utilizar las posiciones preestablecidas de la cámara (tipo 2)" en la página 150)

Asignar una posición fijado de manera predeterminada (en la página 150)

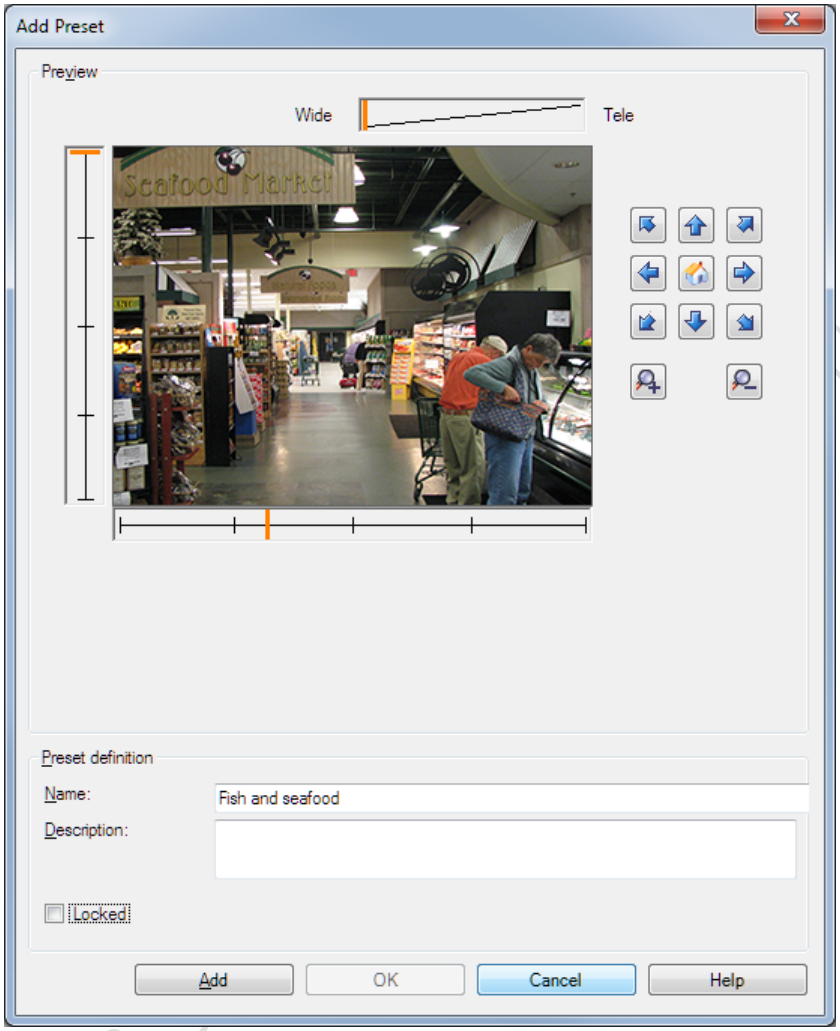
Editar una posición preestablecida (ver "Editar una posición preestablecida (tipo 1 solamente)" en la página 150)

Probar una posición preestablecida (ver "Prueba una posición preestablecida (tipo 1 solamente)" en la página 152)

Añadir una posición preestablecida (tipo 1)

Para añadir una posición preestablecida para la cámara:

1. Haga clic en **Añadir nuevo**. La ventana **Añadir ajuste predeterminado** aparece:



2. La ventana **Añadir valor preestablecido** muestra una imagen de previsualización en directo desde la cámara. Utilice los botones de navegación y / o controles deslizantes para mover la cámara a la posición deseada.
3. Especificar un nombre para la posición predeterminada en el campo **Nombre**.
4. Opcionalmente, escriba una descripción de la posición predeterminada en el campo **Descripción**.
5. Seleccione **Bloqueado** si desea bloquear la posición prefijada. Sólo los usuarios con derechos suficientes pueden desbloquear la posición después.
6. Haga clic en **Añadir** para especificar presintonías. Mantenga la adición hasta que tenga los ajustes preestablecidos que desee.
7. Haga clic en **OK**. La ventana **Añadir valor preestablecido** se cierra, y se suma a la lista de la posición de la **Posiciones preestablecidas** de pestaña de posiciones predefinidas disponibles para la cámara.

Utilizar las posiciones preestablecidas de la cámara (tipo 2)

Como alternativa a la fijación posiciones predefinidas en el sistema, puede especificar posiciones preestablecidas para algunas cámaras PTZ en la propia cámara. Normalmente, puede hacerlo accediendo a una página web de configuración específica del producto.

1. Importar los ajustes predefinidos en el sistema mediante la selección **Utilice los preajustes del dispositivo**.

   Cualquier memoria que haya definido previamente para la cámara se eliminan y se opone a las normas definidas y horarios de patrullaje, así como eliminar los preajustes disponibles para los usuarios de XProtect Smart Client.
2. Haga clic en **Eliminar** a eliminar los predeterminados que sus usuarios no necesitan.
3. Haga clic en **Editar** si desea cambiar el nombre de visualización de la preselección (ver "Editar un nombre posición preestablecida (tipo 2 solamente)" en la página 151).
4. Si más adelante desea modificar dichos ajustes preestablecidos de dispositivos definidos, editar en la cámara y luego volver a importar.

Asignar una posición fijado de manera predeterminada

Si es necesario, puede asignar una de las posiciones predefinidas de una cámara PTZ como la posición por defecto de preajuste de la cámara.

Puede ser útil tener una posición predeterminada por defecto, ya que le permite definir reglas que especifican que la cámara PTZ debe ir a la posición predeterminada por defecto en determinadas circunstancias, por ejemplo después de haber operado la cámara PTZ manualmente.

1. Para asignar una posición predeterminada como el valor predeterminado, seleccione el ajuste preestablecido en su lista de posiciones predeterminadas definidas.
2. Seleccione la casilla de verificación **valor preestablecido predeterminado** debajo de la lista.

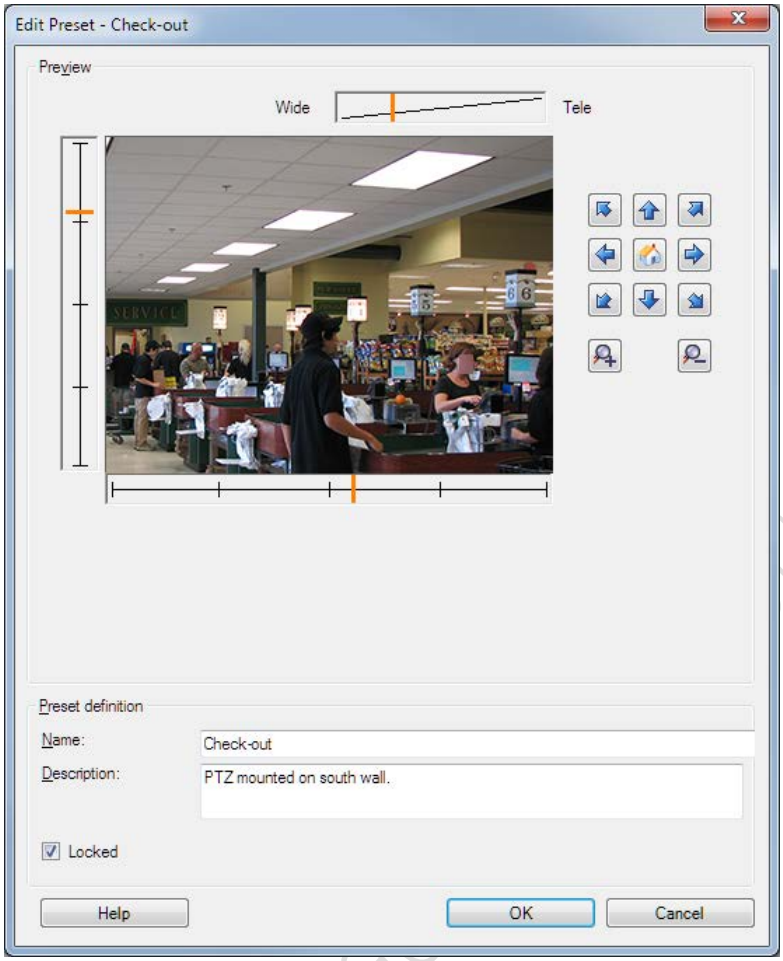
Sólo se puede definir una posición predeterminada como la posición predeterminada por defecto.

Editar una posición preestablecida (tipo 1 solamente)

Para editar una posición preestablecida existente definido en el sistema:

1. Seleccione la posición predeterminada en la lista de la pestaña **Posiciones preestablecidas** de posiciones predefinidas disponibles para la cámara.

2. Haga clic en **Editar**. Esto abre la ventana **Editar Preselección**:



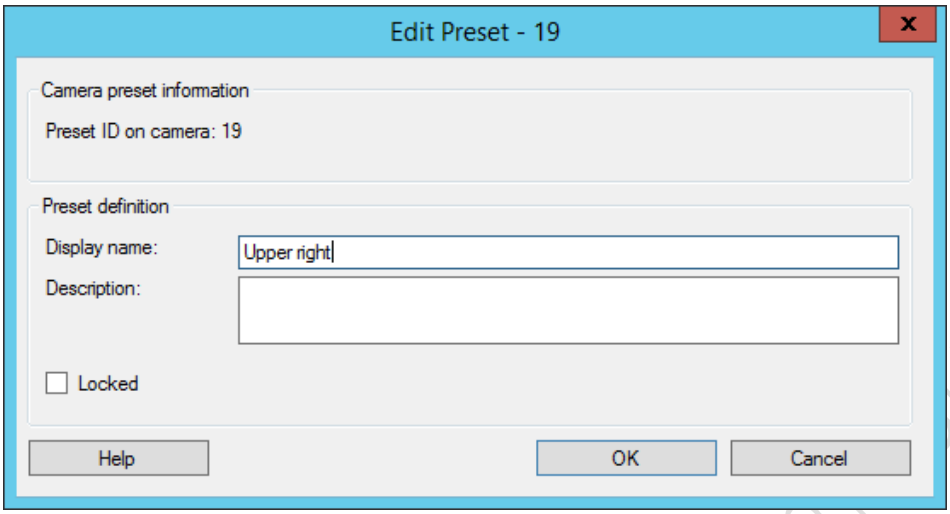
3. La ventana **Editar valor preestablecido** muestra vídeo en directo desde la posición preestablecida. Utilice los botones de navegación y / o controles deslizantes para cambiar la posición preestablecida según sea necesario.
4. Cambiar el nombre / número y descripción de la posición preestablecida si es necesario.
5. Seleccione **Bloqueado** si desea bloquear la posición prefijada. Sólo los usuarios con derechos suficientes pueden desbloquear la posición después.
6. **Haga clic en OK (aceptar)**.

Editar un nombre posición preestablecida (tipo 2 solamente)

Para editar el nombre de una posición preestablecida se define en la cámara:

1. Seleccione la posición predeterminada en la lista de la pestaña **Posiciones preestablecidas** disponibles para la cámara.

2. Haga clic en **Editar**. Esto abre la ventana **Editar Preselección**:



3. Cambiar el nombre y añadir una descripción de la posición preestablecida si es necesario.
4. Seleccione **Bloqueado** si desea bloquear el nombre del preset. Puede bloquear un nombre predefinido si desea evitar que los usuarios de XProtect Smart Client o usuarios con derechos limitados de seguridad de la actualización del nombre del preset o eliminación de la preselección. Los presets bloqueados se indican con este icono . Sólo los usuarios con derechos suficientes pueden desbloquear el nombre preestablecido posteriormente.
5. **Haga clic en OK (aceptar)**.

Bloquear una posición preestablecida

Puede bloquear una posición predeterminada si desea impedir que los usuarios de XProtect Smart Client o usuarios con derechos limitados de seguridad de la actualización o eliminación de un valor preestablecido. Los presets bloqueados se indican con este icono .

Se bloquea preajustes como parte de la adición (ver "Añadir una posición preestablecida (tipo 1)" en la página 149)y editar (ver "Editar una posición preestablecida (tipo 1 solamente)" en la página 150).

Prueba una posición preestablecida (tipo 1 solamente)

1. Seleccione la posición predeterminada en la lista de la pestaña **Posiciones preestablecidas** de posiciones predefinidas disponibles para la cámara.
2. Haga clic en **Activar**.
3. La cámara se mueve a la posición preestablecida seleccionada.

Sesiones PTZ reservadas (explicación)

Según el sistema de vigilancia, puede reservar sesiones PTZ.

Los administradores con derechos de seguridad para ejecutar una sesión PTZ reservada pueden ejecutar la cámara PTZ en este modo. Esto evita que otros usuarios tomen el control de la cámara. En una sesión PTZ, el sistema de prioridad de PTZ se desestima para evitar que usuarios con mayor prioridad interrumpan la sesión.

Puede operar la cámara en una sesión PTZ desde XProtect Smart Client y Management Client.

Reservar una sesión PTZ puede ser útil, so necesita hacer actualizaciones urgentes o realizar mantenimiento de una cámara PTZ o sus valores preestablecidos sin ser interrumpido por otra persona.

No puede iniciar una sesión PTZ reservada si otro usuario con mayor prioridad controla la cámara o si otro usuario ya ha reservado la cámara.

Liberar sesión PTZ

El botón **Liberar** le permite liberar su sesión PTZ actual para que otro usuario pueda controlar la cámara. Al hacer clic **Lanzar**, la sesión PTZ termina inmediatamente y estará disponible para el primer usuario para operar la cámara.

Administradores asignados con el permiso de seguridad **Lanzamiento de la sesión PTZ** tiene los derechos de liberar la sesión PTZ reservada de otros usuarios en cualquier momento. Esto puede, por ejemplo, ser útil en ocasiones en las que necesita para mantener la cámara PTZ o sus ajustes preestablecidos, o si otros usuarios tienen bloqueado accidentalmente la cámara en situaciones de urgencia.

Especificar los tiempos de espera de sesión PTZ

Los usuarios de Management Client y de XProtect Smart Client con los derechos de usuario necesarios pueden interrumpir manualmente el patrullaje de las cámaras PTZ.

Puede especificar cuánto tiempo debe pasar antes de que se reanude el patrullaje periódico para todas las cámaras PTZ en su sistema:

1. Seleccionar **Herramientas** > **Opciones**.
2. En la pestaña **Opciones** de la ventana **general**, seleccione la cantidad de tiempo en el:
   - Lista **Tiempo de espera para las sesiones PTZ manuales** (por defecto es de 15 segundos).
   - Lista **Tiempo de espera para las sesiones de patrullaje pausa** (por defecto es de 10 minutos).
   - Lista **Tiempo de espera para las sesiones de PTZ reservados** (por defecto es de 1 hora).

   Los ajustes se aplican a todas las cámaras PTZ en su sistema.

Puede cambiar los tiempos de espera de forma individual para cada cámara.

1. En el panel de **Navegación del sitio**, haga clic en **Cámara**.
2. En el panel Descripción general, seleccione la cámara.
3. En pestaña **Posiciones preestablecidas**, seleccione la cantidad de tiempo en el:
   - Lista **Tiempo de espera para la lista de sesiones PTZ Manual** (por defecto es de 15 segundos).
   - Lista **Tiempo de espera para una pausa sesión patrullando** (por defecto es de 10 minutos).
   - Lista **Tiempo de espera para la lista de sesiones PTZ reservada** (por defecto es de 1 hora).

   Los ajustes se aplican sólo para esta cámara.

Propiedades de sesión PTZ

La tabla **PTZ sesión** muestra el estado actual de la cámara PTZ.

Nombre	Descripción
Usuario	Muestra el usuario que haya pulsado el botón **reservado** y actualmente controla la cámara PTZ. Si una sesión de patrullaje es activada por el sistema, se muestra **patrullaje**.
Prioridad	Muestra prioridad PTZ del usuario. Sólo se puede asumir el control PTZ sesiones de los usuarios con una prioridad más baja que tú.
Tiempo agotado	Muestra el tiempo restante de la sesión actual del PTZ.
Reservada	Indica si la sesión actual es una sesión de PTZ reservada o no. • **Cierto**; Reservado. • **Falso**; No es reservado.

Puede cambiar los siguientes tiempos de espera para cada cámara PTZ.

Nombre	Descripción
Tiempo de espera para la sesión PTZ Manual	Especificar el período de tiempo de espera para las sesiones de PTZ manuales en esta cámara si desea que el tiempo de espera para ser diferente del período predeterminado. Especificar el período predeterminado en el **Herramientas** menú en **Opciones**.
Tiempo de espera para la sesión PTZ pausa patrullaje	Especificar el período de tiempo de espera para una pausa patrullando sesiones PTZ en esta cámara si desea que el tiempo de espera para ser diferente del período predeterminado. Especificar el período predeterminado en el **Herramientas** menú en **Opciones**.
Tiempo de espera para la sesión reservada PTZ	Especificar el período de tiempo de espera para las sesiones de PTZ reservados en esta cámara si desea que el tiempo de espera para ser diferente del período predeterminado. Especificar el período predeterminado en el **Herramientas** menú en **Opciones**.

Patrullando pestaña (dispositivos)

Pestaña Patrulla (explicada)

Los siguientes dispositivos cuentan con una pestaña **Patrullando**:

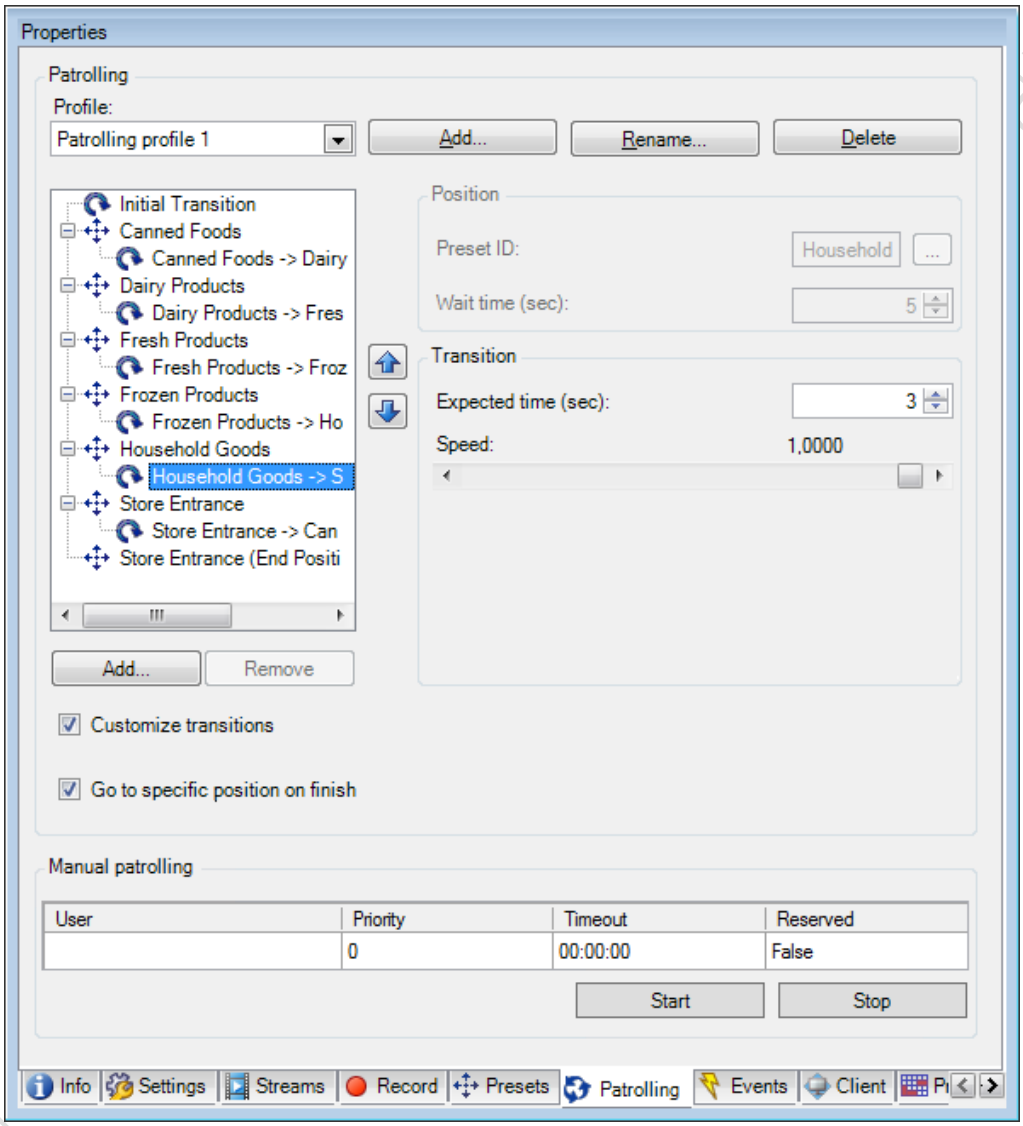
- Cámaras PTZ

En la pestaña **Patrullaje**, puede crear perfiles de patrullaje - el movimiento automático de una cámara PTZ (pan-tilt-zoom) entre un número de posiciones predeterminadas.
Antes de poder trabajar con patrulla, debe especificar al menos dos posiciones preestablecidas para la **Posiciones preestablecidas** pestaña.

Perfiles que patrullan son las definiciones de cómo debe llevarse a cabo patrullaje. Esto incluye el orden en el que la cámara debe moverse entre posiciones predefinidas y el tiempo que debe permanecer en cada posición. Puede crear un número sin restricciones de perfiles de patrullaje y utilizarlos en sus reglas.Por ejemplo, puede crear una regla que especifica que un perfil de patrullaje debe utilizarse durante el horario de atención de día y otra durante las noches.

Antes de aplicar un perfil de patrullaje en una regla, por ejemplo, se puede comprobar el perfil patrullando con patrullaje manual. También puede utilizar el patrullaje manual para hacerse cargo de patrullar de otro usuario o de un patrullaje regla activada, siempre y cuando tenga una prioridad más alta PTZ.

Puede controlar si el sistema está patrullando en la actualidad o que un usuario ha tomado el control, en zona **patrullaje manual**.



Pestaña **Patrulla**, que muestra un perfil de patrulla con transiciones personalizadas.

Añadir un perfil de patrullaje (en la página 156)

Especificar las posiciones predeterminadas en un perfil de patrullaje (en la página 156)

Especificar el tiempo en cada posición preestablecida (en la página 156)

Personalizar transiciones (en la página 157)

Especificar una posición final (en la página 158)

Especificar espera de sesión PTZ manual (ver "Especificar los tiempos de espera de sesión PTZ" en la página 153)

Añadir un perfil de patrullaje

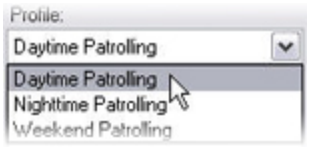
Añadir un perfil que desea utilizar en una regla:

1. Haga clic en **Añadir**. Aparece el cuadro de diálogo **Añadir perfil**.
2. En el cuadro de diálogo **Añadir perfil** , especifique un nombre para el perfil de patrullaje.
3. Haga clic en **OK**. El botón está deshabilitado si el nombre no es único.

   El nuevo perfil de patrulla se agrega a la lista **Perfil**. Ahora puede especificar las posiciones predefinidas y otros ajustes para el perfil de patrullaje.

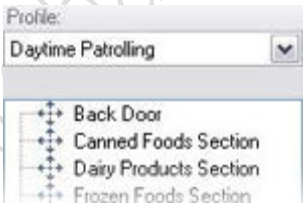
Especificar las posiciones predeterminadas en un perfil de patrullaje

1. Seleccione el perfil que patrulla en lista **Perfil**:



2. Haga clic en **Añadir**.
3. En el cuadro de diálogo **Seleccionar predeterminado**, seleccione las posiciones preestablecidas para su perfil de patrullaje:

4. Haga clic en **OK**. Las posiciones predeterminadas seleccionadas se añaden a la lista de posiciones predefinidas para el perfil de patrullaje:



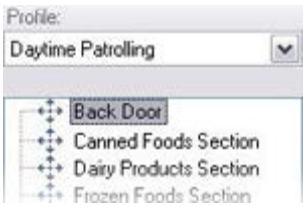
5. La cámara utiliza la posición predeterminada en la parte superior de la lista como la primera parada cuando entra en patrullas de acuerdo con el perfil de patrullaje. La posición predeterminada en la segunda posición de la parte superior es la segunda parada, y así sucesivamente.

Especificar el tiempo en cada posición preestablecida

Cuando el patrullaje, la cámara PTZ de forma predeterminada se mantiene durante 5 segundos en cada posición predeterminada especificada en el perfil de patrullaje.

Para cambiar el número de segundos:

1. Seleccione el perfil de patrullaje en lista **perfil**.
2. Seleccione la posición predeterminada para el que desea cambiar la hora:



3. Especificar el tiempo en el campo **Tiempo en la posición(es)**:
4. Si es necesario, repetir para otras posiciones preestablecidas.

Personalizar transiciones

Por defecto, el tiempo requerido para mover la cámara de una posición preestablecida a otra, conocida como **transición**, se estima en tres segundos. Durante este tiempo, la detección de movimiento está desactivada de forma predeterminada en la cámara, porque de lo contrario es probable que se detecten mientras la cámara se mueve entre las posiciones predefinidas de movimiento irrelevante.

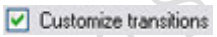
Sólo se puede personalizar la velocidad de las transiciones si su cámara es compatible con PTZ escaneo y es del tipo en posiciones predeterminadas se configuran y se almacenan en el servidor de su sistema (tipo 1 cámara PTZ). De lo contrario la **velocidad** deslizador está en gris.

Puede personalizar lo siguiente:

- El tiempo de transición estimado.
- La velocidad con la que la cámara se mueve durante una transición.

Para personalizar las transiciones entre las diferentes posiciones predefinidas:

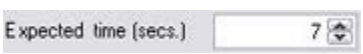
1. Seleccione el perfil de patrullaje en lista **Perfil**.
2. Seleccione casilla de verificación**Personalizar transiciones**:



Indicaciones de transición se añaden a la lista de posiciones predeterminadas.

3. En la lista, seleccione la transición:

4. Especificar el tiempo de transición estimado (en número de segundos) en el campo **el tiempo previsto (s)**:



5. Utilice el deslizador **Velocidad** para especificar la velocidad de transición. Cuando la corredera está en su posición más a la derecha, la cámara se mueve con su velocidad por defecto. Cuanto más se mueva el control deslizante hacia la izquierda, más lenta será la cámara se mueve durante la transición seleccionada.

6. Repita según sea necesario para otras transiciones.

Especificar una posición final

Puede especificar que la cámara debe moverse a una posición predeterminada específica al patrullar acuerdo con los extremos del perfil patrullaje seleccionados.

1. Seleccione el perfil de patrullaje en lista **Perfil**.

2. Seleccione la casilla de verificación **Ir a una posición específica al finalizar**. Esto abre la **Seleccionar predeterminado** cuadro de diálogo.

3. Seleccione la posición final, y haga clic en **OK**.

   Puede seleccionar cualquiera de las posiciones preestablecidas de la cámara como la posición final, usted no está limitado a las posiciones preestablecidas utilizados en el perfil de patrullaje.

4. La posición final seleccionada se añade a la lista de perfiles.

   Cuando el patrullaje de acuerdo a los extremos del perfil patrullaje seleccionados, la cámara se mueve a la posición final especificada.

Patrullaje manual (explicado)

Cuando usted ha diseñado un perfil de patrullaje, puede probar con el patrullaje manual antes de aplicarlo en el sistema. Utilice botones de **inicio** y **parada** para iniciar y detener el patrullaje manual.

Si la cámara ya está patrullando o controlado por otro usuario, sólo se puede iniciar el patrullaje manual si usted tiene una prioridad más alta.

Si se inicia un patrullaje manual mientras la cámara se quede un patrullaje sistema de reglas activado, el sistema volverá a este patrullaje cuando se interrumpe el patrullaje manual. Si otro usuario ejecuta un manual de patrullaje, pero usted tiene una prioridad más alta y comenzar su patrullaje manual, manual de patrullaje del otro usuario no se reanuda.

Si usted no para el manual que patrulla a ti mismo, que continuará hasta que un patrullaje basado en reglas o un usuario con una prioridad más alta se hace cargo. Cuando el patrullaje sistema basado en reglas se detiene, el sistema reanuda su patrullaje manual. Si otro usuario inicia un patrullaje manual, su manual de patrullaje se detiene y no se reanudará.

Cuando se interrumpe el patrullaje manual y que haya definido una posición final para su perfil de patrullaje con **Ir a la posición específica en el acabado**, la cámara vuelve a esta posición.

Propiedades de patrullaje manuales

La tabla **Patrulla manual** muestra el estado actual de la cámara PTZ.

Nombre	Descripción
Usuario	Muestra el usuario que se haya reservado la sesión de PTZ o iniciado un patrullaje manual y actualmente controla la cámara. Si una sesión de patrullaje es activada por el sistema, se muestra **patrullaje**.
Prioridad	Muestra prioridad PTZ del usuario. Sólo se puede asumir el control PTZ sesiones de los usuarios o perfiles que patrullan con una prioridad más baja que la suya.
Tiempo agotado	Muestra el tiempo restante de las sesiones PTZ actuales reservada o manuales.
Reservada	Indica si la sesión actual es una sesión de PTZ reservada o no. • **Cierto**; Reservado. • **Falso**; No es reservado.

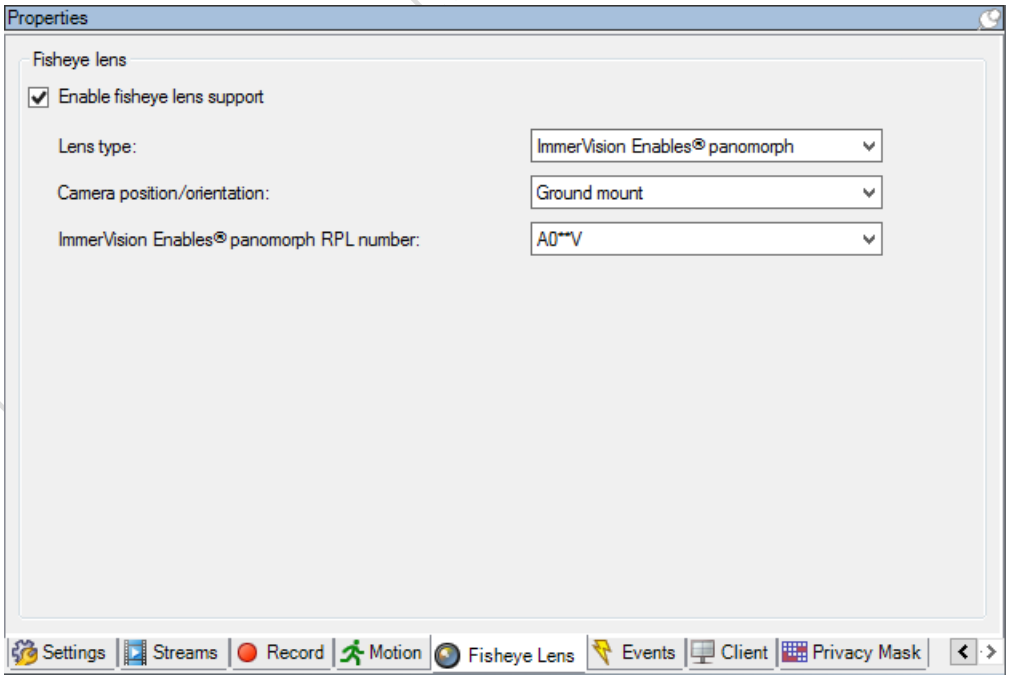
Pestaña lente ojo de pez (dispositivos)

Pestaña Ojo de Pez (explicado)

Los siguientes dispositivos cuentan con una pestaña **Ojo de Pez**:

- Las cámaras fijas con un objetivo ojo de pez

En la pestaña **Objetivo de ojo de pez**, puede habilitar y configurar el soporte de lente fisheye para la cámara seleccionada.



Habilitar y deshabilitar el soporte de objetivo de ojo de pez (en la página 160)

Especificar la configuración de lente ojo de pez (ver "Especificar la configuración de objetivo de ojo de pez" en la página 160)

Habilitar y deshabilitar el soporte de objetivo de ojo de pez

El soporte de objeto de ojo de pez está desactivado por defecto.

Para activarlo o desactivarlo, active o desactive la casilla de verificación de la pestaña **Objetivo de ojo de pez** casilla de verificación **Habilitar soporte para ojo de pez**.

Especificar la configuración de objetivo de ojo de pez

Cuando se habilita el soporte de objetivo de ojo de pez:

1. Seleccionar el tipo de lente.
2. Especificar la posición física / orientación de la cámara de la lista **orientación / posición de la cámara**.
3. Seleccione un número de lente Panomorfo registrado (RPL) de la lista **Número RPL panomorfo de ImmerVision Enables®**.

   Esto asegura la identificación y la configuración correcta de la lente utilizada con la cámara. Usted encuentra generalmente el número de RPL en la lente sí mismo o en la caja en la cual vino. Para obtener más detalles sobre ImmerVision, las lentes panomorfas y los RPL, consulte el sitio web de Immervision **(**https://www.immervisionenables.com/**).**

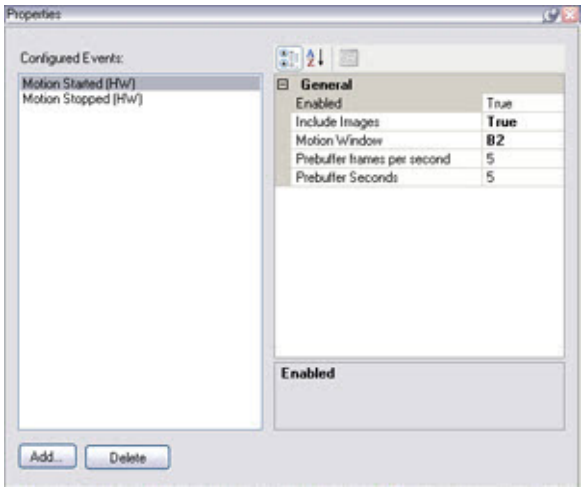
Pestaña de eventos (dispositivos)

Ficha Eventos (explicada)

Los siguientes dispositivos tienen una pestaña **Eventos**:

- Cámaras
- Micrófonos
- Entradas

Además de evento del sistema, algunos dispositivos pueden configurarse para activar eventos. Puede utilizar estos eventos al crear reglas basadas en eventos en el sistema. Técnicamente, se producen en el hardware / dispositivo real en lugar de en el sistema de vigilancia.



Ficha **Evento**, ejemplo de **cámara**.

Cuando se elimina un evento, que afecta a todas las reglas que utilizan el evento.

- Añadir un evento (en la página 161)
- Especificar las propiedades de evento (en la página 161)
- Utilizar varias instancias de un evento (en la página 161)

Añadir un evento

1. En el panel **general**, seleccione un dispositivo.
2. Seleccione la ficha **Eventos** y haga clic en **Añadir**. Esto abre la ventana **Seleccione Controlador de eventos**.
3. Seleccione un evento. Sólo se puede seleccionar un evento a la vez.
4. **Haga clic en OK (aceptar)**.
5. En la barra de herramientas, haga clic en **Guardar**.

Especificar las propiedades de evento

Puede especificar propiedades para cada caso que haya agregado. El número de propiedades depende del dispositivo y el evento. Para que el evento funcione como se pretende, debe especificar algunas o todas las propiedades de forma idéntica en el dispositivo, así como de esta ficha.

Utilizar varias instancias de un evento

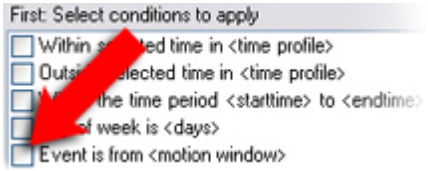
Para ser capaz de especificar diferentes propiedades para diferentes instancias de un evento, puede añadir un evento más de una vez.

El siguiente ejemplo es específico para **cámaras.**

> **Ejemplo**: Ha configurado la cámara con dos ventanas de movimiento, denominadas A1 y A2. Ha agregado dos instancias del evento **Iniciado por movimiento (HW)**. En las propiedades de un caso,

que haya especificado el uso de la ventana de movimiento A1. En las propiedades de la otra instancia, ha especificado el uso de la ventana de movimiento A2.

Cuando se utiliza el evento en una regla, puede especificar que el evento debe basarse en movimiento detectado en una ventana de movimiento específico para que la regla se dispara:



Pestaña evento (propiedades)

Nombre	Descripción
Eventos configurados	Los eventos que puede seleccionar y añadir en la lista **Configurados** se determinan totalmente por el dispositivo y su configuración. Para algunos tipos de dispositivos, la lista está vacía.
General	La lista de propiedades depende del dispositivo y el evento. Para que el evento funcione como se pretende, debe especificar algunas o todas las propiedades de forma idéntica en el dispositivo, así como de esta ficha.

Pestaña Cliente (dispositivos)

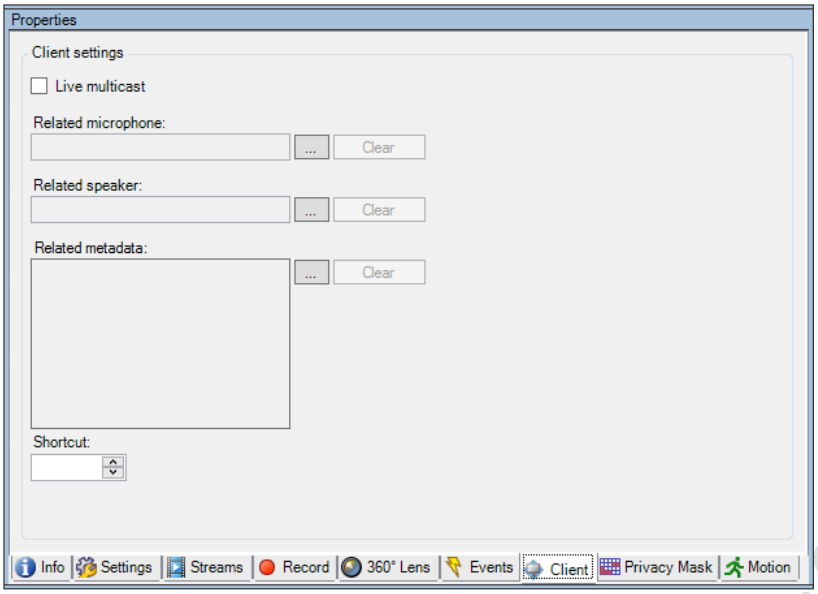
Ficha Cliente (explicada)

Los siguientes dispositivos cuentan con una ficha de **cliente**:

- Cámaras

En la pestaña **Cliente** puede especificar qué otros dispositivos se ven y escuchan cuando utiliza la cámara en XProtect Smart Client.

Los dispositivos relacionados también registran cuando la cámara graba, ver permitir la grabación en dispositivos relacionados (en la página 137).



Propiedades de la ficha cliente

Nombre	Descripción
Multidifusión en directo	El sistema es compatible con la multidifusión de secuencias en vivo desde el servidor de grabación de XProtect Smart Client. Para activar la multidifusión de transmisiones en directo desde la cámara seleccionada, seleccione la casilla de verificación. Tenga en cuenta que la multidifusión en directo sólo funciona en la secuencia que ha especificado como la secuencia predeterminada de la cámara en la ficha **Flujos**. También debe configurar la multidifusión para el servidor de grabación. Ver Multicasting (explicado) (en la página 97). Si las secuencias de multidifusión no funcionan, por ejemplo, debido a las restricciones en la red o en los clientes individuales, el sistema vuelve a la unidifusión.
Micrófono relacionado	Especifican de qué micrófono en la cámara, que los usuarios de XProtect Smart Client reciben por defecto de audio. El usuario XProtect Smart Client puede seleccionar manualmente para escuchar otro micrófono si es necesario **.** El registro micrófonos relacionada cuando la cámara graba.
Altavoz Relacionados	Especifican a través de los altavoces de la cámara, que los usuarios de XProtect Smart Client hablan por defecto. El usuario XProtect Smart Client puede seleccionar manualmente otro orador, si es necesario. Los altavoces relacionados registro cuando la cámara graba.

Nombre	Descripción
Metadatos relacionados	Especificar uno o más dispositivos de metadatos de la cámara, que los usuarios de XProtect Smart Client reciben los datos. El registro de metadatos relacionados con los dispositivos cuando la cámara graba.
Acceso rápido	Para facilitar la selección de cámaras para los usuarios de XProtect Smart Client, definir atajos de teclado para las cámaras. • Crear cada acceso directo por lo que identifica de forma exclusiva a las cámaras. • Un número de acceso directo de la cámara no puede tener más de cuatro dígitos.

Pestaña Máscara de privacidad (dispositivos)

Funcionalidad disponible depende del sistema que está utilizando. Ver tabla de comparación de productos (en la página 24) para más información.

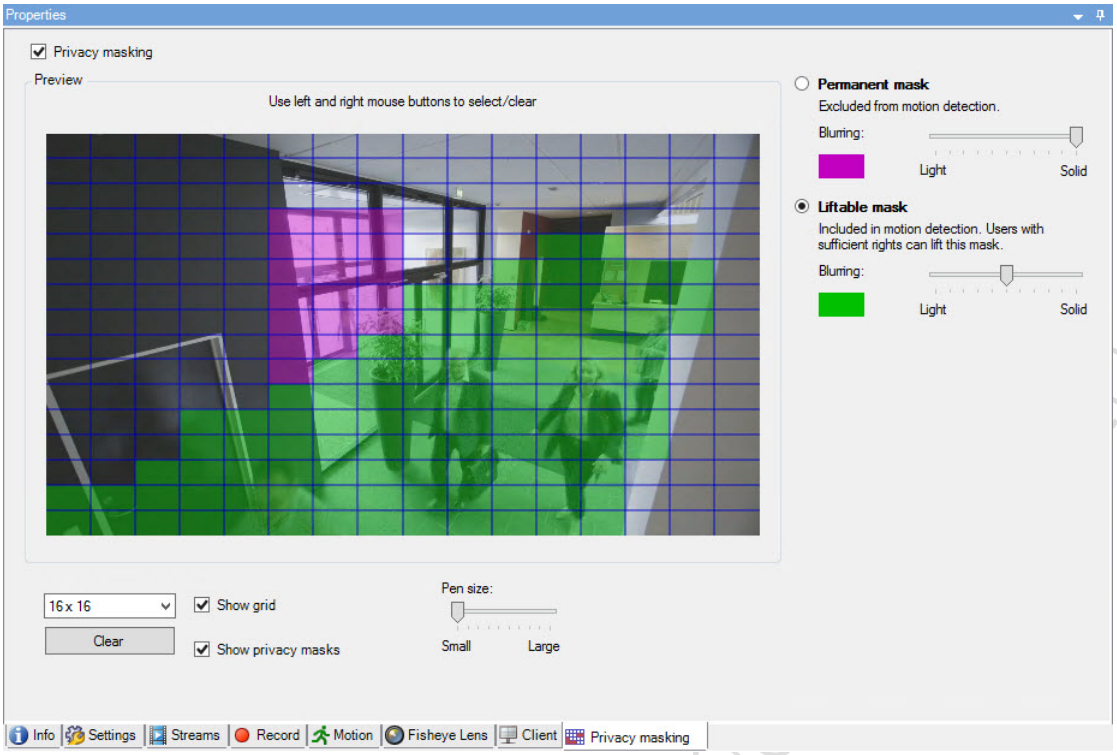
Nota: XProtect Essential+ 2018 R1 en adelante no admite el enmascaramiento de privacidad, por lo que si actualiza desde un sistema con máscaras de privacidad aplicadas, las máscaras serán eliminadas.

Pestaña Máscara de privacidad (explicada)

Los siguientes dispositivos tienen una pestaña **Máscara de privacidad** :

- Cámaras

En la pestaña **Máscara de privacidad** puede habilitar y configurar la protección de privacidad para la cámara seleccionada.



Las máscaras de privacidad se aplican y se bloquean a un área de la imagen de la cámara, por lo que el área cubiertano sigue los movimientos pan-tilt-zoom, sino que cubre constantemente la misma área de la imagen de la cámara. En algunas cámaras PTZ, puede habilitar el enmascaramiento de privacidad basado en posición en la cámara.

En una configuración Milestone Interconnect, el sitio central ignora las máscaras de privacidad definidas en un sitio remoto. Si desea aplicar las mismas máscaras de privacidad, debe redefinirlas en el sitio central.

- Máscara de privacidad (explicado) (en la página 165)
- Activar y desactivar la protección de privacidad (ver "Activar / desactivar Máscara de privacidad" en la página 167)
- Definir máscaras de privacidad (en la página 167)
- Establezca el tiempo de espera para levantar máscaras de privacidad (ver "Cambiar el tiempo de espera para máscaras de privacidad levantadas" en la página 168)
- Dar permiso a los usuarios para levantar máscaras de privacidad (en la página 168)
- Cree un informe de configuración de su configuración de enmascaramiento de privacidad (ver "Crea un informe de tu configuración de enmascaramiento de privacidad " en la página 169)

Máscara de privacidad (explicado)

Con el enmascaramiento de privacidad, puede definir qué áreas del video de una cámara desea cubrir con máscaras de privacidad cuando se muestran en los clientes. Por ejemplo, si una cámara de vigilancia cubre una calle, puede cubrir ciertas áreas de un edificio (pueden ser ventanas y puertas) con máscaras de privacidad, para proteger la privacidad de los residentes. En algunos países, este es un requisito legal.

Puede especificar máscaras de privacidad como sólidas o borrosas. Las máscaras cubren videos en vivo, grabados y exportados.

Hay dos tipos de máscaras de privacidad:

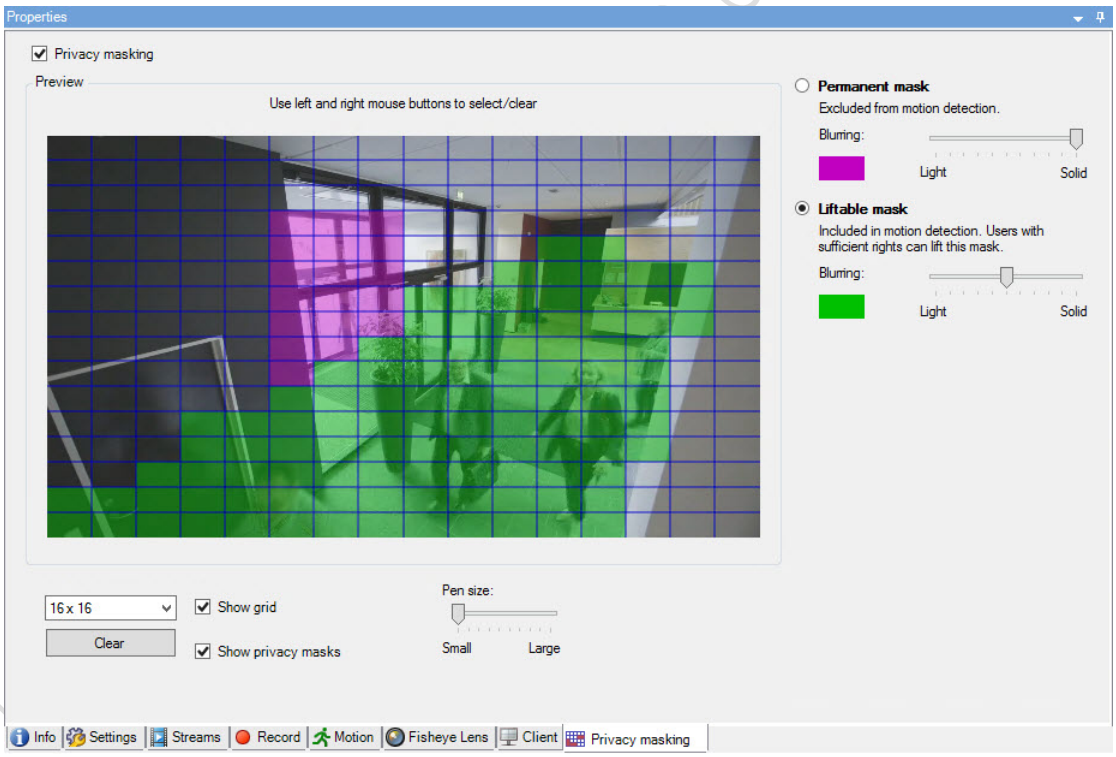
- **Máscara de privacidad permanente**: Las áreas con este tipo de máscara siempre están cubiertas en los clientes. Se puede usar para cubrir áreas del video que nunca requieren vigilancia, como áreas públicas o áreas donde no se permite la vigilancia. La detección de movimiento está excluida de las áreas con máscaras de privacidad permanentes.
- **Máscara de privacidad elevable**: Las áreas con este tipo de máscara pueden ser descubiertas temporalmente en XProtect Smart Client por usuarios con permiso para levantar máscaras de privacidad. Si el usuario registrado XProtect Smart Client no tiene derecho a levantar máscaras de privacidad, el sistema solicita que un usuario autorizado apruebe el levantamiento.
  Las máscaras de privacidad se levantan hasta el tiempo de espera o el usuario las vuelve a aplicar.
  Tenga en cuenta que las máscaras de privacidad se eliminan en video de todas las cámaras a las que el usuario tiene acceso.

Nota: Si actualiza desde un sistema 2017 R3 o anterior con máscaras de privacidad aplicadas, las máscaras se convertirán en máscaras elevables.

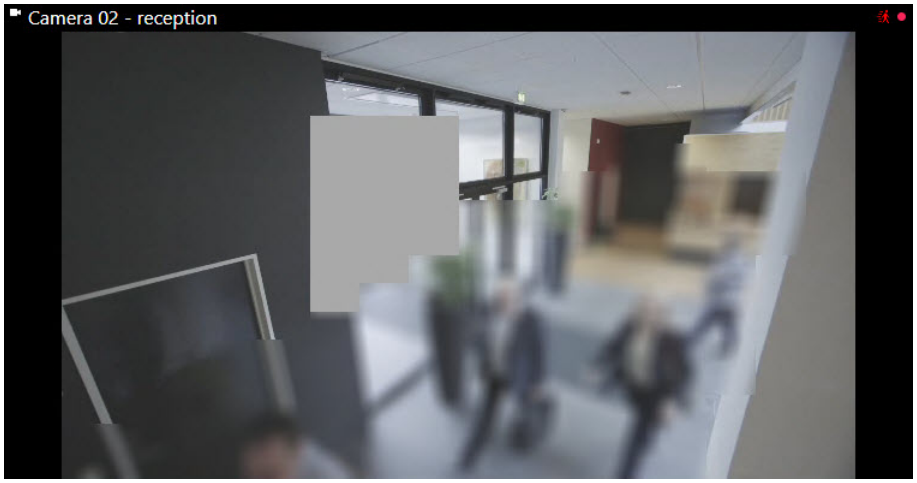
Cuando un usuario exporta o reproduce videos grabados de un cliente, el video incluye las máscaras de privacidad configuradas en el momento de la grabación, incluso si ha cambiado o eliminado las máscaras de privacidad más adelante. Si se quita la protección de privacidad al exportar, el video exportado **no** incluye las máscaras de privacidad elevables.

Importante: Si cambia la configuración de enmascaramiento de privacidad muy a menudo, por ejemplo, una vez a la semana, su sistema puede potencialmente estar sobrecargado.

Ejemplo de pestaña **Máscara de privacidad** con máscaras de privacidad configuradas:



Y así es como aparecen en los clientes:



Nota: Puede informar a los usuarios del cliente sobre la configuración de las máscaras de privacidad permanentes y elevables.

Activar / desactivar Máscara de privacidad

La función de Máscara de privacidad está desactivada por defecto.

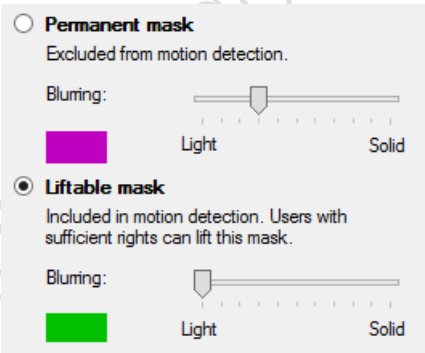
Para activar / desactivar la función Máscara de privacidad para una cámara:

- En la ficha **Máscara de privacidad**, marque o borre casilla de verificación **Máscara de privacidad**.

Definir máscaras de privacidad

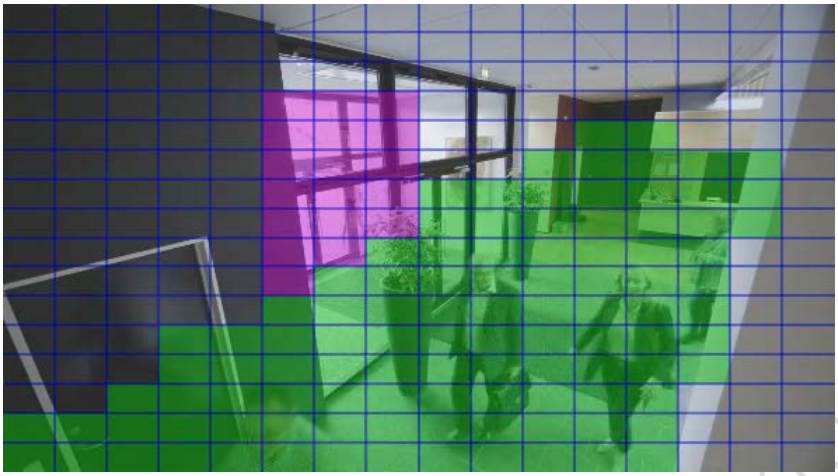
Cuando habilita la función de enmascaramiento de privacidad en la pestaña **Máscara de privacidad** , se aplica una cuadrícula a la vista previa de la cámara.

1. Para cubrir un área con una máscara de privacidad, primero seleccione si desea una máscara de privacidad permanente o elevable.



2. Arrastre el puntero del mouse sobre la vista previa. Presione hacia abajo el botón izquierdo del mouse para seleccionar una celda de cuadrícula. Presione hacia abajo el botón derecho del mouse para borrar una celda de la cuadrícula.

3. Puede definir tantas áreas de máscara de privacidad como sea necesario. Las áreas con máscaras de privacidad permanentes aparecen en morado y las áreas con máscaras de privacidad elevables aparecen en verde.



4. Defina cómo debería aparecer la cobertura de las áreas en el video cuando se muestra en los clientes. Use los controles deslizantes para pasar de una difuminación clara a una máscara completa no transparente.

Nota: Las máscaras de privacidad permanentes también aparecen en la pestaña **Movimiento** .

5. En XProtect Smart Client, verifique que las máscaras de privacidad aparezcan tal como las definió.

Dar permiso a los usuarios para levantar máscaras de privacidad

De forma predeterminada, ningún usuario tiene permisos para levantar máscaras de privacidad en XProtect Smart Client.

Para habilitar / deshabilitar el permiso:

1. Debajo de **Cometidos**, seleccione la función que desea autorizar para levantar las máscaras de privacidad.
2. En la ficha **Seguridad general**, seleccione **Cámaras**.
3. Seleccione la casilla de verificación **Permitir** para permiso **Levantar máscaras de privacidad**.

Los usuarios que asigne a este rol pueden levantar las máscaras de privacidad configuradas como máscaras que se pueden subir para sí mismas y autorizar el levantamiento para otros usuarios de XProtect Smart Client.

Cambiar el tiempo de espera para máscaras de privacidad levantadas

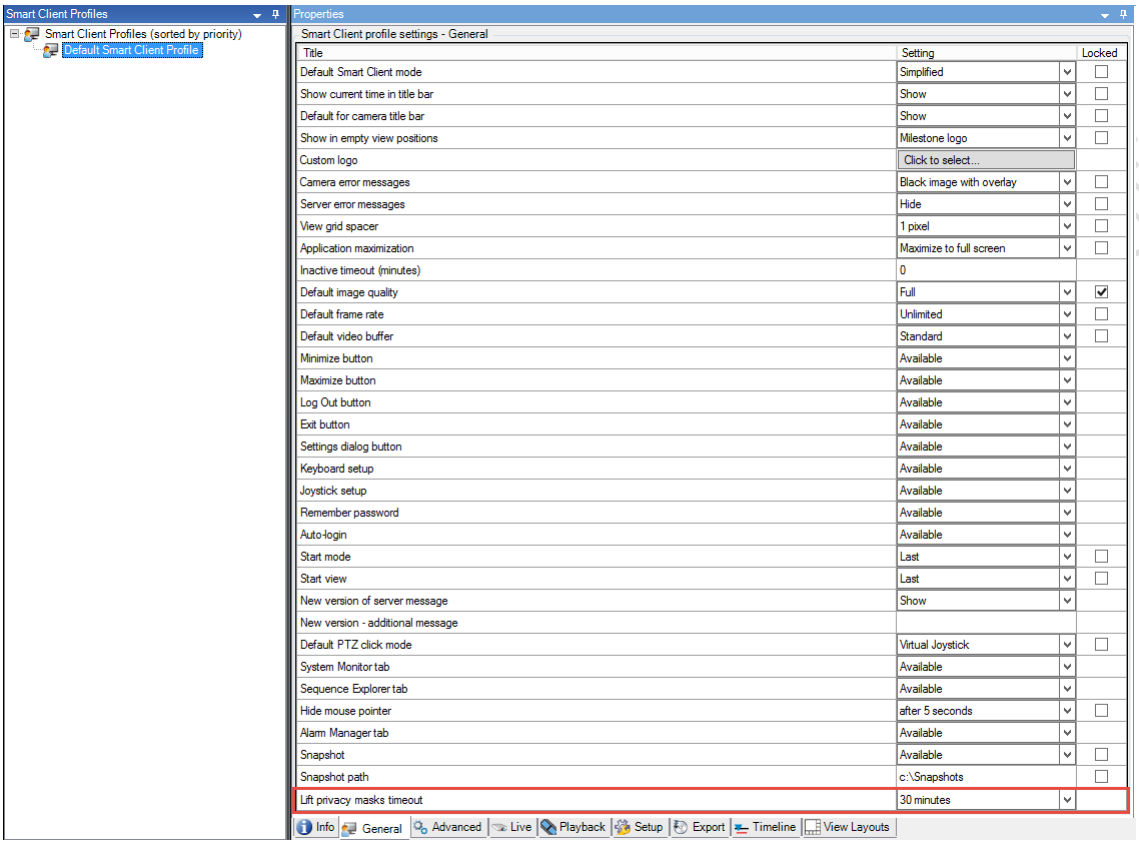
De forma predeterminada, las máscaras de privacidad se levantan durante 30 minutos en XProtect Smart Client y luego se aplican automáticamente, pero puede cambiar eso.

Nota: Cuando cambie el tiempo de espera, recuerde hacerlo para el perfil Smart Client asociado al rol que tiene el permiso para levantar máscaras de privacidad.

Para cambiar el tiempo de espera:

1. Debajo de **Perfiles Smart Client**, seleccione el perfil Smart Client correspondiente.

2. En la ficha **General**, busque **Límite de tiempo para levantar máscaras de privacidad**.



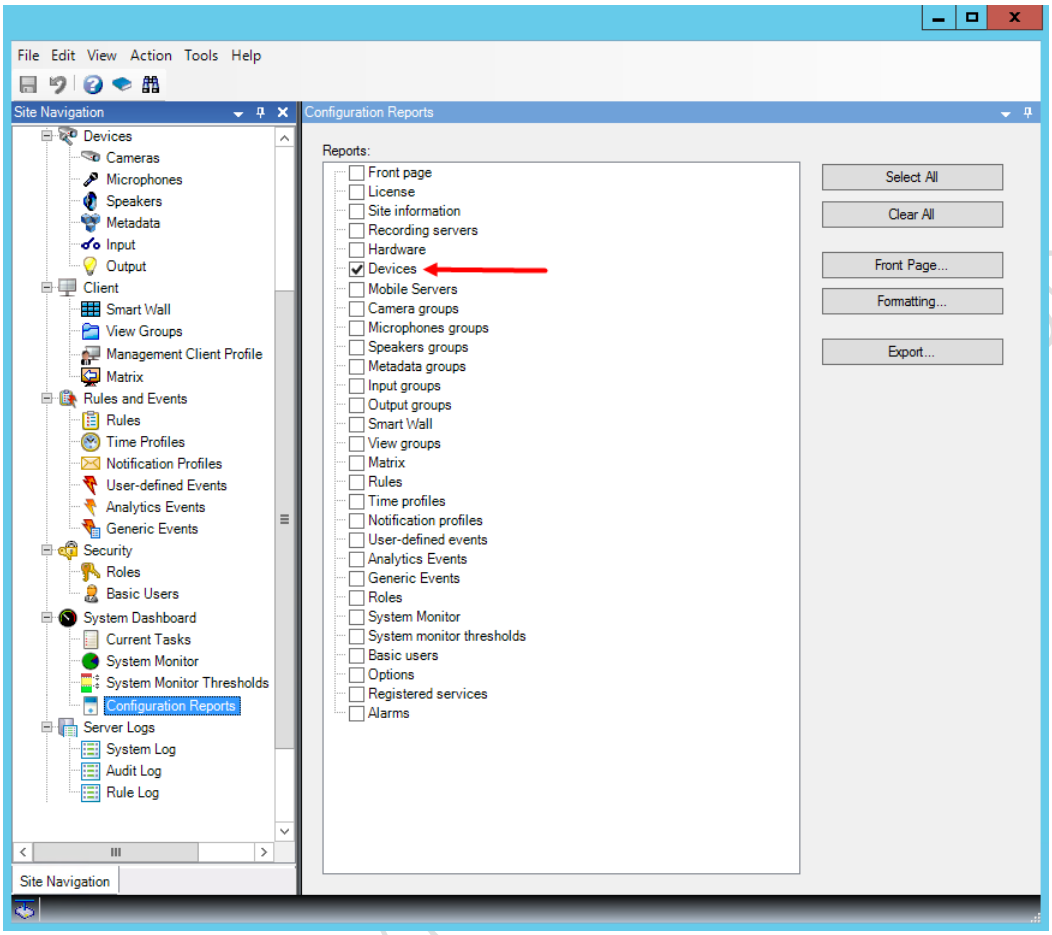
3. Seleccione entre los valores:
   - **2 minutos**
   - **10 minutos**
   - **30 minutos**
   - **1 hora**
   - **2 horas**
   - **Hasta que cierre sesión**
4. Haga clic en **Guardar**.

Crea un informe de tu configuración de enmascaramiento de privacidad

El informe de los dispositivos incluye información sobre la configuración actual de enmascaramiento de privacidad de sus cámaras.

Para configurar un informe:

1. Debajo de **Informes de configuración**, seleccione informe **Dispositivo**.



2. Si desea modificar el informe, puede cambiar la página principal y el formato.
3. Haga clic en **Exportar**, y el sistema crea el informe como un archivo PDF.

Para obtener más información acerca de los informes, consulte Informes de configuración (explicados) (en la página 269).

Pestaña Máscara de privacidad (propiedades)

Nombre	Descripción
Tamaño de la parrilla	El tamaño de cuadrícula seleccionado determina la densidad de la cuadrícula, independientemente de si la cuadrícula está visible en la vista previa o no. Seleccione entre los valores 8×8, 16×16, 32×32 o 64×64.
Limpiar	Borra **todas** las máscaras de privacidad que haya especificado.
Mostrar cuadrícula	Seleccione la casilla de verificación **Mostrar cuadrícula** para hacer visible la cuadrícula.

Nombre	Descripción
Mostrar máscaras de privacidad	Cuando selecciona **Mostrar máscaras de privacidad** casilla de verificación (predeterminado), las máscaras de privacidad permanentes aparecen en color púrpura en la vista previa y las máscaras de privacidad elevables aparecen en color verde. Milestone le recomienda que mantenga seleccionada la casilla **Mostrar máscaras de privacidad** para que usted y sus colegas puedan ver la configuración de protección de privacidad actual.
Tamaño de lápiz	Utilice el deslizador **Tamaño de lápiz** para indicar el tamaño de las selecciones que desea realizar al hacer clic y arrastrar la cuadrícula para seleccionar regiones. El valor predeterminado se establece en pequeño, que es equivalente a un cuadrado en la cuadrícula.
Máscara permanente	Aparece en color morado en la vista previa en esta pestaña y en la pestaña **Movimiento**. Las máscaras de privacidad permanentes siempre están visibles en XProtect Smart Client y no pueden levantarse. Se puede usar para cubrir áreas del video que nunca requieren vigilancia, como áreas públicas, donde no se permite la vigilancia. La detección de movimiento está excluida de las máscaras permanentes. Usted especifica la cobertura de máscaras de privacidad como sólido o algún nivel de borrosa.La configuración de cobertura se aplica tanto al video en vivo como al grabado.
Máscara elevable	Aparece en verde en la vista previa en esta pestaña. Las máscaras de privacidad que se pueden levantar se pueden levantar en XProtect Smart Client por usuarios con suficientes derechos de usuario. De forma predeterminada, las máscaras de privacidad se levantan durante 30 minutos o hasta que el usuario las vuelva a aplicar. Tenga en cuenta que las máscaras de privacidad se eliminan en video de todas las cámaras a las que el usuario tiene acceso. Si el usuario XProtect Smart Client no tiene derecho a levantar máscaras de privacidad, el sistema solicita un usuario con permiso para autorizar el levantamiento. Usted especifica la cobertura de las máscaras de privacidad como sólidas o como borrosas. La configuración de cobertura se aplica tanto al video en vivo como al grabado.
Borrón	Use el control deslizante para seleccionar el nivel de desenfoque de las máscaras de privacidad en los clientes o establezca la cobertura como sólida. Por defecto, la cobertura de áreas con máscaras de privacidad permanentes es sólida (no transparente). De forma predeterminada, las máscaras de privacidad elevables son borrosos medios. Puede informar a los usuarios del cliente sobre la apariencia de las máscaras de privacidad permanentes y elvables, para que puedan distinguir.

Cliente

Clientes (explicado)

Funcionalidad disponible depende del sistema que está utilizando. Ver tabla de comparación de productos (en la página 24) para más información.

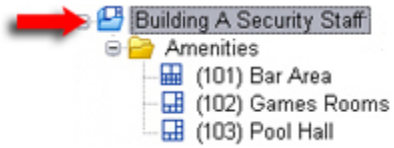
La sección de cliente del Management Client se compone de:

Nombre	Descripción
XProtect Smart Wall	XProtect Smart Wall es un add-on que le permite enviar contenidos vista desde XProtect Smart Client a la pared de vídeo dedicada. Para obtener información más detallada acerca de XProtect Smart Wall, consulte XProtect Smart Wall (explicado (ver "XProtect Smart Wall (explicado)" en la página 322)).
Grupos de vistas	La forma en que se presenta vídeo de las cámaras se llama una vista. Para controlar quién puede ver lo que en XProtect Smart Client, puede crear grupos de vistas a las opiniones del grupo de entidades lógicas. Puede asignar el acceso a estos grupos de vistas a través de cometidos y limitar quién puede acceder a grupos de vistas individuales para cometidos específicas. Seleccione **Grupos de vistas** para diseñar y trabajar con grupos de vistas para que se ajusten a sus necesidades de vigilancia.
Perfiles Smart Client	Para diferenciar a los usuarios XProtect Smart Client, puede crear perfiles de Smart Client, priorizarlos y personalizar sus perfiles según sea necesario para las diferentes tareas a mano.
Perfiles Management Client	Para diferenciar los usuarios administradores de Management Client, puede crear perfiles de Management Client, dar prioridad a estos y personalizar sus perfiles según sea necesario para las diferentes tareas a mano.
Matrix	Matrix es una función para distribuir vídeo de manera remota. Si utiliza la Matrix, se puede insertar vídeo desde cualquier cámara en la red de su sistema a cualquier ejecuta XProtect Smart Client.

Grupos de vistas

Ver grupos (explicados)

La forma en que el sistema presenta el vídeo de una o más cámaras en los clientes se llama una vista. Un grupo de la vista es un contenedor para uno o más grupos lógicos de tales puntos de vista. En los clientes, un grupo de la vista se presenta como una carpeta ampliable a partir del cual los usuarios pueden seleccionar el grupo y la vista que quieren ver:



Ejemplo de XProtect Smart Client: La flecha indica un grupo de la vista, que contiene un grupo lógico (denominados Servicios), que a su vez contiene 3 puntos de vista.

Ver grupos y cometidos (explicado)

De forma predeterminada, cada cometido se define en el Management Client también se crea como un grupo de vistas. Cuando se agrega un cometido en el Management Client, el cometido de forma predeterminada aparece como un grupo de vistas para su uso en los clientes.

- Se puede asignar un grupo de vistas sobre la base de un cometido a los usuarios / grupos asignados al cometido correspondiente. Puede cambiar estos derechos grupo de vistas mediante el establecimiento de esto en el cometido después.
- Un grupo de vistas sobre la base de un cometido lleva el nombre de cometido.

  Ejemplo: Si crea un cometido con el nombre **Personal de Seguridad Edificio A**, aparece en XProtect Smart Client como un grupo de la vista llamada **Personal de Seguridad Edificio A**.

  Además de los grupos de vistas que se obtienen al añadir cometidos, puede crear tantos otros grupos de vistas a su gusto. También puede eliminar grupos de vistas, incluyendo los creados automáticamente al añadir cometidos.
- Incluso si se crea un grupo de la vista cada vez que se agrega un cometido, ver los grupos no tienen que corresponden a los cometidos. Puede añadir, renombrar o eliminar cualquiera de los grupos de vistas, si es necesario.

Tenga en cuenta que si cambia el nombre de un grupo de vistas, los usuarios de clientes ya conectados deben desconectarse y conectarse de nuevo antes de que el cambio de nombre es visible.

Añadir un grupo de vistas

1. Haga clic con el botón secundario del mouse en **Grupos de vistas** y seleccione **Añadir Grupo de vistas**. Esto abre la **Añadir grupo de vistas** cuadro de diálogo.
2. Escriba el nombre y una descripción opcional del nuevo grupo de la vista y haga clic en **OK**.

Nota: No hay cometidos tienen derecho a utilizar el grupo de la vista que acaba de añadir hasta que haya especificado tales derechos. Si ha especificado qué cometidos que pueden utilizar el grupo de vista recién añadido, los usuarios de clientes que ya están conectadas con los cometidos pertinentes deben desconectarse y conectarse de nuevo antes de que puedan ver el grupo de vistas.

Perfiles Smart Client

Perfiles Smart Client (explicados)

Funcionalidad disponible depende del sistema que está utilizando. Ver tabla de comparación de productos (en la página 24) para más información.

Los perfiles de Smart Client permiten a los administradores de sistemas para controlar cómo XProtect Smart Client debe verse y comportarse y qué características y paneles de usuarios XProtect Smart Client tener acceso. Puede configurar derechos de usuario para: paneles y opciones, minimizar / maximizar las opciones de inactividad, control de tiempo, recordar contraseña o no, vista mostrada después de iniciar la sesión, el diseño de impresión de informes, ruta de exportación, y mucho más.

Para administrar perfiles Smart Client en el sistema, expanda **Cliente** y seleccione **Perfiles Smart Client**. Usted también puede aprender acerca de la relación entre perfiles de Smart Client, cometidos y perfiles temporales y cómo utilizar estos juntos (ver "Creación y configuración de perfiles Smart Client, cometidos y perfiles temporales" en la página 174).

Añadir y configurar un perfil de Smart Client

Debe crear un perfil de Smart Client antes de poder configurarlo.

1. Clic con el botón derecho **Perfiles de Smart Client**.
2. Seleccione **Añadir Perfil Smart Client**.
3. En el cuadro de diálogo **Añadir Perfil Smart Client**, escriba un nombre y una descripción del nuevo perfil y haga clic en **OK**.
4. En el panel **general**, haga clic en el perfil que ha creado para configurarlo.
5. Ajustar la configuración de una, varias o todas las fichas disponibles y haga clic en **OK**.

Copiar un perfil de Smart Client

Si usted tiene un perfil de Smart Client con ajustes o derechos complicados y necesitan un perfil similar, podría ser más fácil de copiar un perfil ya existente y hacer ajustes menores a la copia que a la creación de un nuevo perfil a partir de cero.

1. Haga clic **perfiles de Smart Client**, haga clic en el perfil en el panel **general**, seleccione **Copiar perfil de Smart Client**.
2. En el cuadro de diálogo que aparece, dar el perfil copiado un nuevo nombre único y una descripción. **Haga clic en OK (aceptar)**.
3. En el panel **Descripción general**, haga clic en el perfil que acaba de crear para configurarlo. Esto se realiza mediante la configuración de ajuste en una, varias o todas las fichas disponibles. **Haga clic en OK (aceptar)**.

Creación y configuración de perfiles Smart Client, cometidos y perfiles temporales

Cuando se trabaja con perfiles de Smart Client, es importante comprender la interacción entre los perfiles de Smart Client, cometidos y perfiles temporales.

- Smart Client perfiles de acuerdo con los ajustes correctos de usuario en XProtect Smart Client
- Los cometidos se ocupan de la configuración de seguridad de los clientes, MIP SDK y más

- Perfiles temporales de acuerdo con los aspectos temporales de los dos tipos de perfiles

En conjunto, estas tres características proporcionan un control único y la personalización de posibilidades con respecto a los derechos de los usuarios de XProtect Smart Client.

Ejemplo: Es necesario un usuario en la configuración de XProtect Smart Client, que sólo se debe permitir ver vídeo en directo (sin reproducción) de las cámaras seleccionadas, y sólo durante las horas de trabajo normales (8,00 a 16:00). Una forma de configurar esto podría ser como sigue:

1. Crear un perfil de Smart Client, y el nombre, por ejemplo, **Solo en directo**.
2. Especifique la configuración en vivo / reproducción necesarios sobre **único** vivo.
3. Crear un perfil temporal, y el nombre, por ejemplo, **sólo durante el día**.
4. Especificar el período de tiempo que se necesita en la **Sólo durante el día**.
5. Crear un nuevo cometido y el nombre, por ejemplo, la Guardia **(cámaras seleccionadas)**.
6. Especifique qué cámaras **Guardia (cámaras seleccionadas)** puede utilizar.
7. Asignar el perfil Smart Client **única vivo** y el perfil temporal **Sólo durante el día** de el cometido **Guardia (cámaras seleccionadas)** para conectar los tres elementos.

Ahora tiene una mezcla de las tres características que crean el resultado deseado y dejando espacio para una fácil puesta a punto y ajustes. Observe también que no puede realizar la configuración en un orden diferente, por ejemplo, creando el cometido primero y luego el perfil de Smart Client y el perfil temporal, o de cualquier otro orden que prefiera.

Ajuste el modo simplificado como el modo por defecto

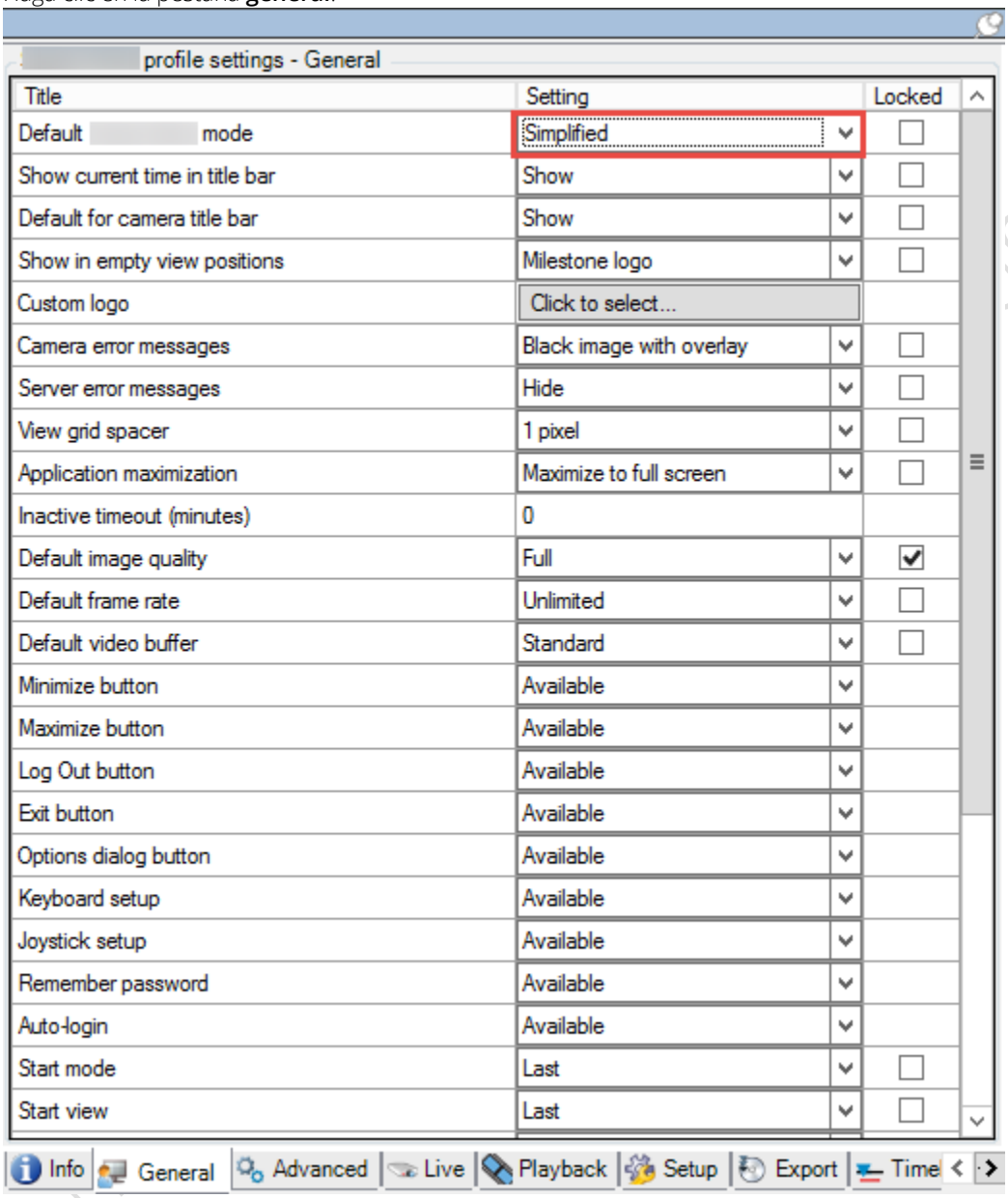
A través de los perfiles de Smart Client, puede configurar el sistema para abrir automáticamente XProtect Smart Client en modo simplificado con un conjunto limitado de funciones y las pestañas. De forma predeterminada, XProtect Smart Client se abre en el modo avanzado con el conjunto completo de funciones y pestañas.

Si el operador XProtect Smart Client en algún momento decide cambiar a un modo diferente que el modo por defecto, XProtect Smart Client recuerda este ajuste, la próxima vez que el operador abre el programa.

1. En Management Client, expanda el nodo **cliente**.

2. Seleccione el perfil de Smart Client relevante.

3. Haga clic en la pestaña **general**.



4. En la lista **modo por defectoSmart Client**, seleccione **Simplificado**. XProtect Smart Client se abre ahora en el modo simplificado para los usuarios asociados con el perfil de Smart Client actual.

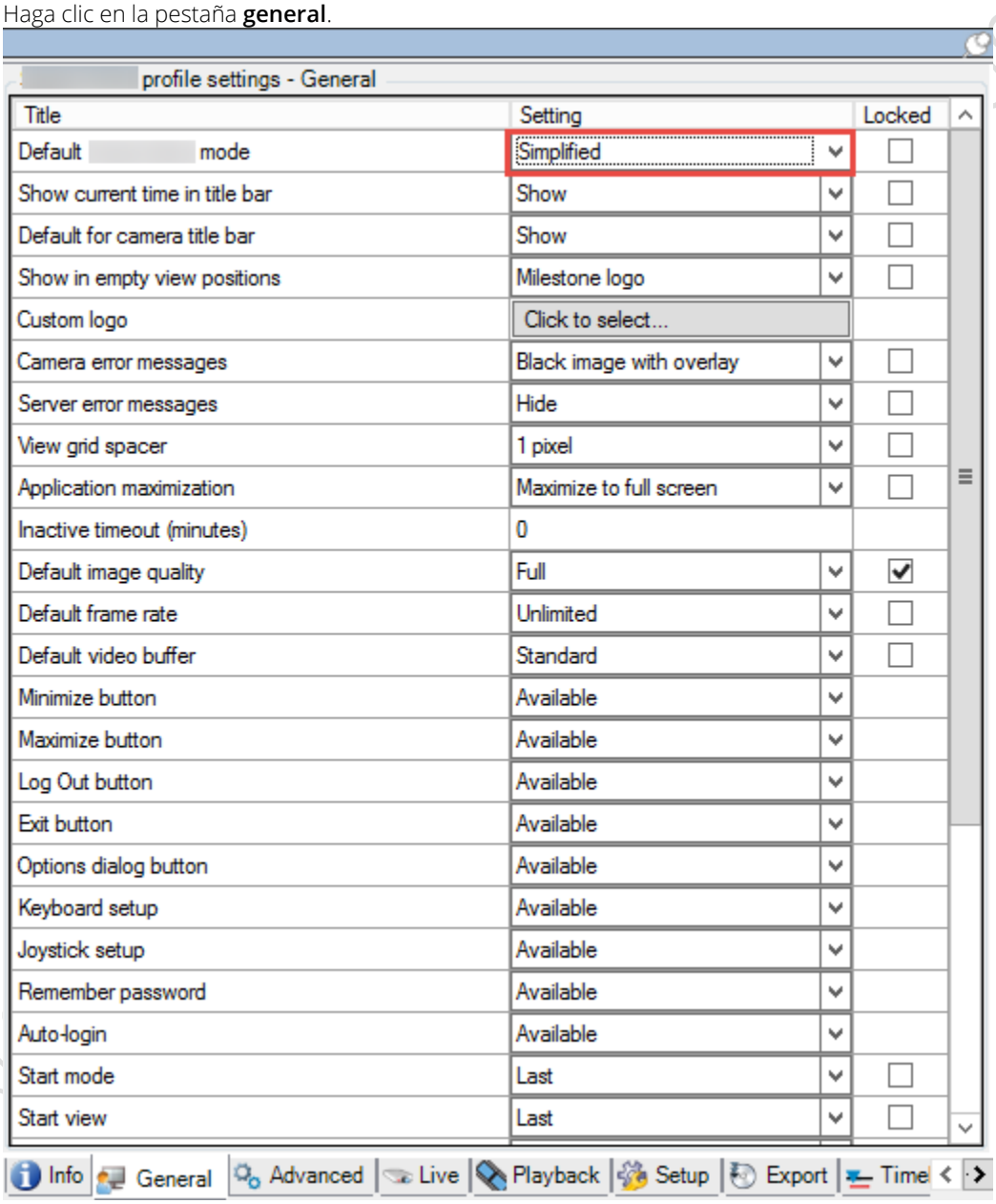
Ver también

Los operadores no podrán cambiar entre el modo simple y avanzada (en la página 177)

Los operadores no podrán cambiar entre el modo simple y avanzada

En XProtect Smart Client, los operadores pueden cambiar entre el modo simple y avanzada. Sin embargo, puede evitar que los operadores de XProtect Smart Client desde la conmutación entre modos. Técnicamente, debe bloquear la configuración que determina si XProtect Smart Client se abre en modo simple o modo avanzado.

1. En Management Client, expanda el nodo **cliente**.
2. Seleccione el perfil de Smart Client relevante.
3. Haga clic en la pestaña **general**.



4. Compruebe que la lista **Modo Smart Client predeterminado** tiene el valor adecuado. Si **Habilitado**, XProtect Smart Client se abre en el modo sencillo.
5. Seleccione la casilla de verificación **Bloqueada**. El botón de modo de alternar en XProtect Smart Client está oculto.

Ver también

El modo sencillo establecer como el modo por defecto (ver "Ajuste el modo simplificado como el modo por defecto" en la página 175)

Propiedades de perfil de Smart Client

Las siguientes fichas le permiten especificar las propiedades de cada perfil de Smart Client. Puede bloquear la configuración del Management Client, si es necesario, por lo que los usuarios de XProtect Smart Client no se pueden cambiar:

Pestaña	Descripción
Información	Nombre y descripción, prioridad de los perfiles existentes y una visión general de los cometidos que utilizan el perfil. Si un usuario es miembro de más de una función, cada uno con su perfil de Smart Client individual, el usuario obtiene el perfil de Smart Client con la más alta prioridad.
General	Ajustes como mostrar / ocultar y mini- y maximizar la configuración del menú, login / -out, inicio, tiempo de espera, información y opciones de mensajería, y la configuración del Explorador de Secuencias.
Avanzados	Ajustes avanzados tales como hilos de decodificación máximos, el desentrelazado y la configuración de zona horaria. **Bandas de decodificación máxima** controla cuántos hilos de descodificación se utilizan para decodificar secuencias de vídeo. Puede ayudar a mejorar el rendimiento en los ordenadores de varios núcleos en vivo, así como el modo de reproducción. La mejora exacta rendimiento depende de la secuencia de vídeo. Es especialmente relevante si se utilizan secuencias de vídeo de alta resolución en gran medida codificados como H. 264 / H. 265, para lo cual el potencial de mejora del rendimiento puede ser significativo, y menos relevante si se utiliza, por ejemplo, JPEG o MPEG-4. Con **Desentrelazando**, convertir vídeo en un formato no entrelazado. El entrelazado determina cómo una imagen se actualiza en una pantalla. La imagen se actualiza mediante el escaneo de las líneas impares primero en la imagen, a continuación, la exploración de las líneas pares. Esto permite una mayor velocidad de actualización, ya que menos información se procesa durante cada barrido. Sin embargo, en algunas situaciones el entrelazado puede causar parpadeo, o los cambios en que sólo se advierten la mitad de las líneas de la imagen para cada escaneo.
Directo	Disponibilidad de fichas/paneles en vivo, reproducción de cámaras y botones de superposición, cuadros delimitadores y plug-ins relacionados con Live-related MIP.
Reproducción	Disponibilidad de las pestañas / paneles de reproducción, disposición de los informes de impresión, reproducción independiente, marcadores, cuadros delimitadores y complementos MIP relacionados con la reproducción.

Pestaña	Descripción
Configuración	Disponibilidad de la configuración general / paneles / botones, plug-in de configuración MIP y derechos para editar un mapa y editar el almacenamiento en tiempo real de vídeo.
Exportaciones	Caminos, máscaras de privacidad, formatos de vídeo y de imágenes fijas y qué incluir al exportar estos, formatos de exportación para XProtect Smart Client – Player y mucho más.
Línea temporal	Si se debe incluir o no el audio, la visibilidad de la indicación de tiempo y movimiento, y, finalmente, cómo manejar las lagunas de reproducción. También puede seleccionar si desea mostrar datos adicionales o marcadores adicionales de otras fuentes.
Control de acceso	Seleccione si las notificaciones de solicitud de acceso deben aparecer en la pantalla de XProtect Smart Client cuando son activados por eventos.
Plano Inteligente	Especifique la configuración de la función Mapa inteligente. Puede especificar si OpenStreetMaps está disponible para su uso como fondo geográfico y si XProtect Smart Client creará automáticamente ubicaciones cuando un usuario añada una superposición personalizada al mapa inteligente. También puede especificar la frecuencia con la que desea que el sistema borre los datos relacionados con Smart Maps de su computadora. Para ayudar a que XProtect Smart Client muestre Smart Map más rápido, el cliente guarda los datos del mapa en la caché de su computadora. Con el tiempo esto podría ralentizar su computadora. Si desea utilizar Bing Maps o Google Maps como fondos geográficos, introduzca una clave para una API de Bing Maps o una clave privada y un ID de cliente para la API de Google Static Maps.

Perfiles Management Client

Perfiles Management Client (explicados)

Funcionalidad disponible depende del sistema que está utilizando. Ver tabla de comparación de productos (en la página 24) para más información.

Los perfiles de clientes de gestión permiten a los administradores del sistema para modificar la interfaz de usuario de Management Client para otros usuarios. Los perfiles de Management Client asociados con cometidos para limitar la interfaz de usuario para representar la funcionalidad disponible para cada cometido de administrador.

Para asociar un rol con un perfil Management Client, vea la pestaña Información (ver "Pestaña Información (cometidos)" en la página 232) de Configuración de cometido. Tenga en cuenta que los perfiles de Management Client sólo manejan la representación visual de la funcionalidad del sistema, no el acceso real a la misma. Para limitar el acceso general a la funcionalidad del sistema para un cometido, consulte la ficha seguridad general (ver "Pestaña de Seguridad General (cometidos)" en la página 234) de Configuración de cometido.

Puede cambiar la configuración de la visibilidad de todos los elementos de Management Client. Por defecto, el perfil de Management Client puede ver toda la funcionalidad del Management Client.

- Para limitar la visibilidad de la funcionalidad, desactive las casillas de verificación de la funcionalidad correspondiente a fin de eliminar la funcionalidad visualmente desde el Management Client para cualquier usuario de Management Client con un cometido asociado con este perfil de Management Client.

Aparte del cometido de administrador integrada, sólo los usuarios asociados con un cometido que se le ha concedido **administrar la seguridad** permisos para el servidor de gestión en la pestaña **Seguridad general**, puede añadir, editar y borrar perfiles de Management Client.

Añadir y configurar un perfil de Management Client

Si no desea utilizar el perfil predeterminado, puede crear un perfil de Management Client antes de poder configurarlo.

1. Clic con el botón derecho **Perfiles de Management Client**.
2. Seleccione **Añadir perfiles de Management Client**.
3. En el **Añadir Perfil Management Client** cuadro de diálogo, escriba un nombre y una descripción del nuevo perfil y haga clic en **OK**.
4. En el panel **general**, haga clic en el perfil que ha creado para configurarlo.
5. En la ficha **Perfil**, active o desactive la funcionalidad del perfil de Management Client.

Copiar un perfil de Management Client

Si usted tiene un perfil de Management Client con los ajustes que le gustaría volver a utilizar, puede copiar un perfil ya existente y realizar pequeños ajustes en la copia en lugar de crear un nuevo perfil a partir de cero.

1. Haga clic en **perfil de Management Client**, haga clic en el perfil en el panel **general**, seleccione **Copiar perfile de Management Client**.
2. En el cuadro de diálogo que aparece, dar el perfil copiado un nuevo nombre único y una descripción. **Haga clic en OK (aceptar)**.
3. En el panel **general**, haga clic en el perfil y vaya a la pestaña **Información** o pestaña **Perfil** para configurar el perfil.

Propiedades de perfil de Management Client

Pestaña de información (perfiles de Management Client)

En la pestaña **información**, puede establecer los siguientes perfiles de Management Client:

Componente	Requisitos
Nombre	Introduzca un nombre para el perfil de Management Client.
Prioridad	Utilice las flechas arriba y abajo para establecer una prioridad para el perfil de Management Client.
Descripción	Introduzca una descripción para el perfil. Esto es opcional.
Cometidos utilizando el perfil de Management Client	Este campo muestra los cometidos que usted ha asociado con el perfil de Management Client. No puede editar esto.

Pestaña perfil (perfiles de Management Client)

Funcionalidad disponible depende del sistema que está utilizando. Ver tabla de comparación de productos (en la página 24) para más información.

En la pestaña **Perfil**, puede activar o desactivar la visibilidad de los siguientes elementos de interfaz de usuario del Management Client:

Navegación

En esta sección, decidir si se permite que un usuario administrador asociado con el perfil de Management Client para ver las distintas características y funcionalidad situados en el panel de **navegación**.

Elemento de navegación	Descripción
Conceptos básicos	Permite al usuario administrador asociado con el perfil de Management Client para ver **Información de licencia** y **Información del sitio**.
Servicios de conexión remota	Permite al usuario administrador asociado con el perfil Management Client ver **Axis One-click Camera Conexión**.
Servidores	Permite al usuario administrador asociado con el perfil de Management Client para ver **servidores de grabación** y **Servidores failover**.
Dispositivos	Permite al usuario administrador asociado con el perfil de Management Client para ver **Cámaras**, **Micrófonos**, **Altavoces**, **Metadatos**, **Entrada** y **Salida** .
Cliente	Permite al usuario administrador asociado con el perfil de Management Client para ver **Smart Wall**, **Grupos de vistas**, **Perfiles de Smart Client**, **Perfiles de Management Client** y **Matrix**.
Reglas y eventos	Permite al usuario administrador asociado con el perfil de Management Client para ver **Reglas**, **Perfiles Temporal**, **los perfiles de notificación**, **Eventos definidos por el usuario**, **Eventos de analytics** y **Eventos genéricos**.
Seguridad	Permite al usuario administrador asociado con el perfil de Management Client para ver **Cometidos** y **usuarios básicos**.
Panel del sistema	Permite al usuario administrador asociado con el perfil de Management Client para ver **Monitor de sistema**, **Umbrales del monitor del sistema**, **Bloqueo de evidencias**, **Tareas actuales** y **Informes de configuración**.
Registros de servidores	Permite al usuario administrador asociado con el perfil de Management Client para ver **Registro del sistema**, **Registro de auditorías** y **Registro de reglas**.
Control de acceso	Permite al usuario administrador asociado con el perfil de Management Client para ver **control de acceso** características, si ha añadido integraciones de sistemas de control de acceso o plug-ins para su sistema.

Detalles

En esta sección, decidir si se permite que un usuario administrador asociado con el perfil de Management Client para ver las distintas fichas para un canal específico del dispositivo, por ejemplo, pestaña **ajustes** o pestaña **Registro** para las cámaras.

Canal de dispositivo	Descripción
Cámaras	Permite al usuario administrador asociado con el perfil de Management Client para ver algunos o todos los ajustes y las pestañas relacionadas con la cámara.
Micrófonos	Permite al usuario administrador asociado con el perfil de Management Client para ver algunos o todos los ajustes y las pestañas relacionadas con micrófono.
Altavoces	Permite al usuario administrador asociado con el perfil de Management Client para ver algunos o todos los ajustes y las pestañas relacionados con los altavoces.
Metadatos	Permite al usuario administrador asociado con el perfil de Management Client para ver algunos o todos los ajustes y las pestañas relacionadas con metadatos.
Entrada	Permite al usuario administrador asociado con el perfil de Management Client para ver algunos o todos los ajustes y las fichas de entrada relacionada.
Salida	Permite al usuario administrador asociado con el perfil de Management Client para ver algunos o todos los ajustes y las pestañas relacionados con la producción.

Menú Herramientas

En esta sección, decidir si se permite que un usuario administrador asociado con el perfil de Management Client para ver los elementos que forman parte de menú **herramientas**.

La opción de menú de herramientas	Descripción
Servicios registrados	Permite al usuario administrador asociado con el perfil de Management Client para ver **servicios registrados**.
Cometidos eficaces	Permite al usuario administrador asociado con el perfil de Management Client para ver **Cometidos eficaces**.
Opciones	Permite al usuario administrador asociado con el perfil de Management Client para ver **Opciones**.
Servidores Enterprise	Permite al usuario administrador asociado con el perfil de Management Client para ver los **servidores Enterprise**.

Sitios federados

En esta sección, decidir si se permite que un usuario administrador asociado con el perfil de Management Client para ver la panel de **jerarquía de sitios federados**.

Matrix

Matrix (explicado)

Con Matrix, puede enviar vídeo desde cualquier cámara en una red que opera el sistema de Matrix-receptores. Un receptor Matrix es un equipo que puede mostrar vídeo activada por Matrix. Hay dos tipos de receptores de la Matrix:

- los equipos que ejecutan una aplicación Matrix dedicada y
- equipos que ejecutan XProtect Smart Client.

Para ver una lista de Matrix destinatarios configurados en el Management Client, expanda **Cliente** en el panel de **Navegación del sitio** y, a continuación, seleccione **Matrix**. Una lista de configuraciones Matrix se muestra en el panel **Propiedades**.

Cada destinatario de Matrix, sin tener en cuenta si se trata de un equipo con la Matrix Monitor o el XProtect Smart Client, debe estar configurado para recibir vídeo Matrix por alarma. Consulte la documentación del Matrix Monitor y XProtect Smart Client para obtener más información.

Añadir destinatarios de Matrix

Para añadir un destinatario de la Matrix existente, por ejemplo, un Matrix Monitor existente o instalación de XProtect Smart Client, a través del Management Client:

1. Expandir **clientes**, a continuación, seleccione **Matrix**.
2. Haga clic en **Configuraciones Matrix** y seleccione **Añadir Matrix**.
3. Rellene los campos de la **Añadir Matrix** cuadro de diálogo.
4. En el campo **Dirección** introduzca la dirección IP o el nombre de host del destinatario Matrix requerido.
5. En el campo **Puerto** ingrese el número de puerto utilizado por la instalación del destinatario Matrix. Puede encontrar el número de puerto y la contraseña de esta manera: Para una aplicación Matrix Monitor, vaya al cuadro de diálogo Matrix Monitor **Configuración**. Para XProtect Smart Client, consulte la documentación de XProtect Smart Client.
6. **Haga clic en OK (aceptar)**.

Ahora puede utilizar el receptor Matrix en reglas.

Nota: Su sistema no verifica que el número de puerto o la contraseña especificada es correcta o que el número de puerto, la contraseña o tipo especificado corresponde con el destinatario de Matrix real. Asegúrese de que introduce la información correcta.

Definir reglas de envío de vídeo a Matrix-receptores

Para enviar vídeo a Matrix-receptores debe incluir el receptor Matrix en una regla que desencadena la transmisión de vídeo a la relacionada Matrix-receptor. Para ello:

1. En el **Navegación del sitio** panel, Expandir **Reglas y eventos** > **Reglas**. Haga clic con el botón secundario del mouse en **Reglas** para abrir el asistente **Administrar regla**. En el primer paso, seleccione un tipo de regla y en la segunda etapa, una condición.
2. En **Administrar regla** paso 3 (**Paso 3: Acciones**) Seleccione el **Conjunto de Matrix para ver los <dispositivos>** acción.

3. Haga clic en el enlace de Matrix en la descripción inicial regla.
4. En el cuadro de diálogo **Seleccione configuración Matrix**, seleccione la Matrix-receptor correspondiente y haga clic en **OK**.
5. Haga clic en los **dispositivos** enlace en la descripción inicial de la regla y seleccione una de las cámaras que se desea enviar vídeo a la Matrix-receptor, a continuación, haga clic en **Aceptar** para confirmar su selección.
6. Haga clic en **Finalizar** si la regla es completa o definir si las acciones adicionales que se requieren y / o una acción de parada.

Si elimina una Matrix-receptor, cualquier regla que incluye la Matrix-receptor deja de funcionar.

Enviar el mismo vídeo a varios puntos de vista de XProtect Smart Client

Si el recipiente Matrix es XProtect Smart Client, puede enviar el mismo vídeo a las posiciones de la Matrix en varias de las opiniones de XProtect Smart Client, siempre y posiciones de la Matrix las visitas comparten el mismo número de puerto y la contraseña:

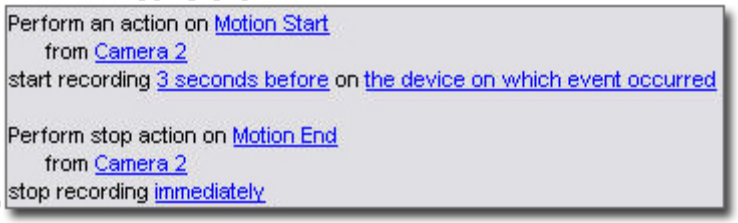
1. En XProtect Smart Client, cree los puntos de vista relevantes y posiciones de la Matrix que comparten el mismo número de puerto y la contraseña.
2. En el Management Client, añadir el correspondiente XProtect Smart Client como Matrix-receptor.
3. Puede incluir la Matrix-receptor en una regla.

Reglas y eventos

Reglas y eventos (explicado)

Las reglas son un elemento central en su sistema. Reglas determinan la configuración de gran importancia, como cuando las cámaras deben registrar, cuando las cámaras PTZ deben patrullar, cuando las notificaciones deben ser enviadas, etc.

Ejemplo: una regla que especifica que una cámara en particular debería comenzar a grabar cuando detecta movimiento:



Los eventos son elementos centrales cuando se utiliza el asistente **Gestionar regla**. En el asistente, los eventos se utilizan principalmente para activar las acciones **.** Por ejemplo, puede crear una regla que especifica que en **evento** del movimiento detectado, el sistema de vigilancia debe tener la **acción** de iniciar la grabación de vídeo de una cámara en particular.

Dos tipos de condiciones pueden desencadenar reglas:

Nombre	Descripción
Eventos	Cuando ocurren eventos en el sistema de vigilancia, por ejemplo, cuando se detecta movimiento o el sistema recibe la entrada de sensores externos.
Hora	Cuando se introduce períodos específicos de tiempo, por ejemplo: `Jueves 16 de agosto de 2007 a la 07.00 07,59` o `todos los sábados y domingos`.

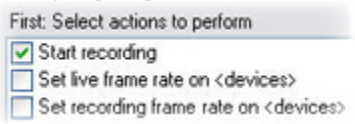
Puede trabajar con el punto siguiente **Reglas y Eventos**:

- **Reglas:** Las reglas son un elemento central en el sistema. El comportamiento de su sistema de vigilancia está en gran medida determinada por reglas. Al crear una regla, se puede trabajar con todo tipo de eventos.
- **Perfiles temporales:** Perfiles temporales son periodos de tiempo definidos en el Management Client. Los utiliza cuando se crea reglas del Management Client, por ejemplo, para crear una regla que especifica que una determinada acción debe tener lugar dentro de un perfil temporal determinado.
- **Perfiles de notificación:** Puede utilizar los perfiles de notificación para configurar notificaciones por correo electrónico ya preparadas, las cuales se pueden activar de forma automática por regla general, por ejemplo, cuando se produce un evento en particular.
- **Eventos definidos por el usuario:** Eventos definidos por el usuario son hechos a la medida que hace posible que los usuarios activen manualmente los acontecimientos en el sistema o reaccionan a las entradas del sistema.
- **Eventos analiticos**: Eventos analíticos son los datos recibidos a partir de un análisis de contenido de vídeo de terceros externa (VCA) proveedores. Puede usar los eventos de analytics como base para las alarmas.
- **Eventos genéricos:** Eventos genéricos le permiten activar acciones en el servidor de eventos XProtect mediante el envío de cadenas simples a través de la red IP para su sistema.

Consulte Visión general Eventos (en la página 194) para obtener una lista de eventos.

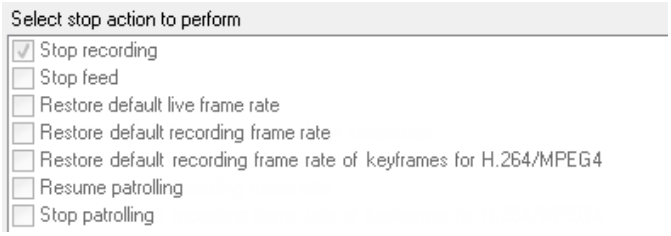
Acciones y acciones de detención (explicadas)

Cuando agrega reglas (ver "Añadir una regla" en la página 208) en el asistente **Gestionar regla**, puede seleccionar entre diferentes acciones:



Algunas de las acciones requieren una acción de parada. **Ejemplo**: Si selecciona la acción **Iniciar grabación**, la grabación comienza y potencialmente continúa indefinidamente. Como resultado, la acción **Iniciar grabación** tiene una acción de parada obligatoria llamada **detener la grabación**.

El asistente **Gestionar Regla** se asegura que especifique acciones de detención cuando sea necesario:



Selección de acciones de detención. En el ejemplo, tenga en cuenta la acción de parada obligatoria (seleccionado, atenuado), las acciones no relevantes de tope (atenuado) y las acciones de detención opcional (seleccionable).

Cada tipo de acción de su sistema XProtect se describe. Es posible que tenga más acciones disponibles si la instalación de sistema utiliza productos complementarios o plug-ins específicos del proveedor. Para cada tipo de acción, información de la acción del autobús aparece en su caso:

Acción	Descripción
Iniciar grabación en <dispositivos>	Empezar a grabar y guardar los datos en la base de datos de los dispositivos seleccionados. Cuando seleccione este tipo de acción, el asistente para la **Gestionar regla** le pedirá que especifique: Cuando la grabación debe comenzar. Esto sucede inmediatamente o una serie de segundos antes de que el evento desencadenante / comienzo del intervalo de tiempo de activación y en la que los dispositivos de la acción deben tener lugar. Este tipo de acción requiere que se haya activado la grabación de los dispositivos a los que se vincula la acción. Sólo se puede guardar los datos antes de un intervalo de tiempo de eventos o si se ha activado pre-buffering para los dispositivos pertinentes. Habilita la grabación y especificar los ajustes pre-buffering para un dispositivo en la ficha de **registro**. **Se requiere una acción de detención**: Este tipo de acción requiere una o más acciones de detención. En uno de los siguientes pasos, el asistente le pedirá automáticamente que especifique la acción de detención: **Detener grabación**. Sin esta acción de parada, grabación potencialmente podría continuar indefinidamente. También tiene la opción de especificar aún más acciones de detención.
Iniciar directo en <dispositivos>	Comience datos alimentar desde los dispositivos en el sistema. Cuando se inicia la alimentación de un dispositivo, los datos se transfieren desde el dispositivo al sistema, en cuyo caso se puede ver y grabar, en función del tipo de datos. Cuando selecciona este tipo de acción, el asistente **Gestionar Regla** le pide que especifique en qué dispositivos iniciar los feeds. El sistema incluye una regla predeterminada que asegura que los alimentos siempre se ponen en marcha en todas las cámaras. **Se requiere una acción de detención**: Este tipo de acción requiere una o más acciones de detención. En uno de los siguientes pasos, el asistente le pedirá automáticamente que especifique la acción de detención: **Detener directo**. También puede especificar otras acciones de detención. Tenga en cuenta que con la acción de parada obligatoria **Detener alimentación** para detener la alimentación de un dispositivo significa que los datos ya no se

Acción	Descripción
	transfieren desde el dispositivo al sistema, en cuyo caso ya no es posible ver y grabar en directo el vídeo. Sin embargo, un dispositivo en el que haya detenido la alimentación todavía puede comunicarse con el servidor de grabación, y se puede iniciar la alimentación de nuevo de forma automática a través de una norma, a diferencia de cuando se ha desactivado manualmente el dispositivo. **Importante:** Si bien este tipo de acciones permite el acceso a fuentes de datos de dispositivos seleccionados, esto no garantiza que se registra los datos, ya que debe especificar la configuración de grabación por separado.
Poner <Smart Wall> a <preestablecido>	Establece el XProtect Smart Wall a un preajuste seleccionado. Especificar la memoria en la pestaña **Valores preestablecidos de Smart Wall**. **Ninguna acción de parada obligatoria**: Este tipo de acción no requiere una acción de detención. Puede especificar acciones de detención opcional que se deben realizar en cualquiera de un evento o después de un período de tiempo.
Establezca <Smart Wall> <monitor> para mostrar <cameras>	Establece un XProtect Smart Wall específica monitor para visualizar vídeo en directo desde las cámaras seleccionadas en este sitio o cualquier sitio secundario configurado en Milestone Federated Architecture. **Ninguna acción de parada obligatoria**: Este tipo de acción no requiere una acción de detención. Puede especificar acciones de detención opcional que se deben realizar en cualquiera de un evento o después de un período de tiempo.
Poner <Smart Wall> <monitor> para mostrar el texto <mensajes>	Establece un XProtect Smart Wall específica monitor para visualizar un mensaje de texto definido por el usuario de hasta 200 caracteres. **Ninguna acción de parada obligatoria**: Este tipo de acción no requiere una acción de detención. Puede especificar acciones de detención opcional que se deben realizar en cualquiera de un evento o después de un período de tiempo.
Eliminar <cameras> de <Smart Wall> monitor <monitor>	Impedir que se muestren vídeo de una cámara específica. **Ninguna acción de parada obligatoria**: Este tipo de acción no requiere una acción de detención. Puede especificar acciones de detención opcional que se deben realizar en cualquiera de un evento o después de un período de tiempo.
Ajustar velocidad de fotogramas de directo a <dispositivos>	Establece una velocidad de fotogramas en particular para utilizar cuando las pantallas del sistema de vídeo en directo de las cámaras seleccionadas que sustituye velocidad de fotogramas predeterminada de las cámaras. Especificar esto en la pestaña **Configuración**. Cuando selecciona este tipo de acción, el Asistente para la **Gestionar regla** le pide que especifique qué velocidad de fotogramas se debe establecer y en qué dispositivos. Siempre verifique que la velocidad de fotogramas que especifique está disponible en las cámaras correspondientes. **Se requiere una acción de detención**: Este tipo de acción requiere una o más acciones de detención. En uno de los siguientes pasos, el asistente le pedirá automáticamente que especifique la acción de detención: **Restaurar velocidad predefinida de fotogramas de directo**. Sin esta acción de parada, la velocidad de fotogramas predeterminada potencialmente podría no ser restaurado. También tiene la opción de especificar aún más acciones de detención.
Ajustar velocidad de	Establece una velocidad de fotogramas particular, a utilizar cuando el sistema guarda

Acción	Descripción
fotogramas de grabación en <dispositivos>	el vídeo grabado por las cámaras seleccionadas en la base de datos, en lugar de la velocidad de fotogramas de grabación por defecto de las cámaras. Al seleccionar este tipo de acción, el asistente **Gestionar regla** le pedirá que especifique qué velocidad de grabación para ajustar, y en el que las cámaras. Sólo se puede especificar una velocidad de grabación para JPEG, un códec de vídeo con el que cada cuadro se comprime por separado en una imagen JPEG. Este tipo de acción también requiere que se haya activado la grabación de las cámaras a la que se vincula la acción. Se habilita la grabación de una cámara en la pestaña **Registro**. La velocidad máxima que puede especificar depende de los tipos de cámaras pertinentes, y en su resolución de imagen seleccionado. **Se requiere una acción de detención**: Este tipo de acción requiere una o más acciones de detención. En uno de los siguientes pasos, el asistente le pedirá automáticamente que especifique la acción de detención: **Restaurar velocidad predefinida de fotogramas de grabación**. Sin esta acción de parada, la velocidad de fotogramas de grabación por defecto potencialmente podría no ser restaurado. También tiene la opción de especificar aún más acciones de detención.
Ajustar velocidad de fotogramas de grabación en todos los fotogramas para MPEG-4/H.264/H.265 en <dispositivos>	Establece la frecuencia de imagen para grabar todos los marcos cuando el sistema guarda el vídeo grabado por las cámaras seleccionadas en la base de datos, en lugar de sólo los fotogramas clave. Permitir a los fotogramas clave de grabación única función en la pestaña **Registro**. Al seleccionar este tipo de acción, el asistente **Gestionar regla** le solicita que seleccione los dispositivos que la acción debe solicitar. Sólo se puede activar la grabación fotograma clave para MPEG-4/H.264/H.265. Este tipo de acción también requiere que se haya activado la grabación de las cámaras a la que se vincula la acción. Se habilita la grabación de una cámara en la pestaña **Registro**. **Se requiere una acción de detención**: Este tipo de acción requiere una o más acciones de detención. En uno de los siguientes pasos, el asistente le pedirá automáticamente que especifique la acción de detención: **Restaurar velocidad de fotogramas clave predeterminada de grabación para MPEG-4/H.264/H.265** Sin esta acción de parada, la configuración por defecto potencialmente no ser restaurado. También tiene la opción de especificar aún más acciones de detención.

Acción	Descripción
Comience patrullando en <dispositivo> usando <perfil> PTZ con prioridad <prioridad>	Empieza PTZ patrullando según un perfil de patrullaje particular para una cámara en particular PTZ con una prioridad particular. Esta es una definición exacta de cómo patrullaje debe llevarse a cabo, incluyendo la secuencia de posiciones predeterminadas, la configuración de sincronización, y mucho más. Si ha actualizado su sistema desde una versión anterior del sistema, los valores antiguos (**Muy bajo**, **Bajo**, **Medio**, **Alta** y **Muy Alta**) se han traducido de la siguiente manera: • = Muy Baja 1000 • Bajo = 2000 • Medio = 3000 • A = 4000 • Muy Alta = 5000 Cuando selecciona este tipo de acción, el Asistente **Gestionar regla** le solicita que seleccione un perfil de patrullaje. Sólo se puede seleccionar un perfil de patrullaje en un dispositivo y no se puede seleccionar varios perfiles de patrullaje. Este tipo de acción requiere que los dispositivos a los que se vincula la acción son dispositivos PTZ. Debe definir al menos un perfil de patrullaje para el dispositivo (s). Usted define patrullando perfiles para una cámara PTZ en la ficha **Patrullaje**. **Se requiere una acción de detención**: Este tipo de acción requiere una o más acciones de detención. En uno de los siguientes pasos, el asistente le pedirá automáticamente que especifique la acción de detención: **Detener patrulla** Sin esta acción de parada, patrullaje potencialmente no dejar nunca. También puede especificar otras acciones de detención.
Detener patrulla en <dispositivos>	Pausas PTZ patrullando. Al seleccionar este tipo de acción, el asistente **Gestionar regla** le pide que especifique los dispositivos en los que hacer una pausa en el patrullaje. Este tipo de acción requiere que los dispositivos a los que se vincula la acción son dispositivos PTZ. Debe definir al menos un perfil de patrullaje para el dispositivo (s). Usted define patrullando perfiles para una cámara PTZ en la ficha **Patrullaje**. **Se requiere una acción de detención**: Este tipo de acción requiere una o más acciones de detención. En uno de los siguientes pasos, el asistente le pedirá automáticamente que especifique la acción de detención: **Reanudar patrulla** Sin esta acción de parada, patrullaje potencialmente podría hacer una pausa indefinida. También tiene la opción de especificar aún más acciones de detención.
Mover <dispositivo> a <preestablecido> posición con prioridad	Mueve una cámara en particular a una posición predeterminada en particular - sin embargo siempre de acuerdo a la prioridad. Al seleccionar este tipo de acción, el Asistente **Gestionar regla** le solicita que seleccione una posición preestablecida. Sólo una posición predeterminada en una cámara puede ser seleccionado. No es

Acción	Descripción
PTZ <prioridad>	posible seleccionar varias posiciones predefinidas. Este tipo de acción requiere que los dispositivos a los que se vincula la acción son dispositivos PTZ. Esta acción requiere que haya definido al menos una posición preestablecida para esos dispositivos. Se definen las posiciones preestablecidas para una cámara PTZ en la pestaña **Valores preestablecidos**. **Ninguna acción de parada obligatoria**: Este tipo de acción no requiere una acción de detención. Puede especificar acciones de detención opcional que se deben realizar en cualquiera de un evento o después de un período de tiempo.
Mover al fijado de manera predeterminada en <dispositivos> PTZ con prioridad <prioridad>	Mueve uno o más particulares cámaras a sus respectivas posiciones predefinidas por defecto - sin embargo siempre de acuerdo a la prioridad. Al seleccionar este tipo de acción, el asistente **Gestionar regla** le solicita que seleccione los dispositivos que la acción debe solicitar. Este tipo de acción requiere que los dispositivos a los que se vincula la acción son dispositivos PTZ. Esta acción requiere que haya definido al menos una posición preestablecida para esos dispositivos. Se definen las posiciones preestablecidas para una cámara PTZ en la pestaña **Valores preestablecidos**. **Ninguna acción de parada obligatoria**: Este tipo de acción no requiere una acción de detención. Puede especificar acciones de detención opcional que se deben realizar en cualquiera de un evento o después de un período de tiempo.
Ajustar salida de dispositivo a <estado>	Establece una salida en un dispositivo a un estado particular (activada o desactivada). Cuando selecciona este tipo de acción, el asistente **Gestionar regla** le pide que especifique qué estado establecer y en qué dispositivos. Este tipo de acción requiere que los dispositivos a los que la acción está vinculada cada uno tiene al menos una unidad de salida externa conectada a un puerto de salida. **Ninguna acción de parada obligatoria**: Este tipo de acción no requiere una acción de detención. Puede especificar acciones de detención opcional que se deben realizar en cualquiera de un evento o después de un período de tiempo.
Crear marcador en <dispositivo>	Crea un marcador en la transmisión en vivo o grabaciones de un dispositivo seleccionado. Un marcador hace que sea fácil volver sobre un determinado evento o período de tiempo. Los ajustes de marcadores se controlan desde el cuadro de diálogo **Opciones**. Al seleccionar este tipo de acción, el asistente **Gestionar regla** le pide que especifique detalles del marcador y seleccione los dispositivos. **Ninguna acción de parada obligatoria**: Este tipo de acción no requiere una acción de detención. Puede especificar acciones de detención opcional que se deben realizar en cualquiera de un evento o después de un período de tiempo.

Acción	Descripción
Reproducir <mensaje> de audio en <dsipoitivos> con <prioridad>	Reproduce un mensaje de audio en los dispositivos seleccionados disparados por un evento.Los dispositivos son en su mayoría altavoces o cámaras. Este tipo de acción requiere que haya cargado el mensaje en el sistema en **Herramientas** > **Opciones** > **Mensajes de audio** ficha. Puede crear más reglas para el mismo evento y enviar mensajes diferentes a cada dispositivo, pero siempre según la prioridad.Las prioridades que controlan la secuencia son las establecidas en la regla y en el dispositivo para un cometido en la ficha **Discurso**: • Si se reproduce un mensaje y se envía otro mensaje con la misma prioridad al mismo altavoz, se completa el primer mensaje y luego se inicia el segundo. • Si se reproduce un mensaje y se envía otro mensaje con mayor prioridad al mismo altavoz, el primer mensaje se interrumpe y el segundo se inicia inmediatamente.
Enviar notificación a <perfil>	Envía una notificación, con un perfil de notificación en particular. Cuando selecciona este tipo de acción, el Asistente **Gestionar regla** le solicita que seleccione un perfil de notificación y qué dispositivos incluirán imágenes de prealarma. Sólo se puede seleccionar un perfil de notificación y no se puede seleccionar varios perfiles de notificación. Tenga en cuenta que un único perfil de notificación puede contener varios destinatarios. También puede crear más reglas para el mismo evento y enviar diferentes notificaciones a cada uno de los perfiles de notificación. Puede copiar y volver a utilizar el contenido de reglas haciendo clic con el botón secundario en una regla en la lista **Reglas**. Este tipo de acción requiere que haya definido al menos un perfil de notificación. Imágenes pre-alarma sólo se incluyen si se ha habilitado la opción **incluir imágenes** para el perfil de notificación correspondiente. **Ninguna acción de parada obligatoria**: Este tipo de acción no requiere una acción de detención. Puede especificar acciones de detención opcional que se deben realizar en cualquiera de un evento o después de un período de tiempo.
Crear nueva <entrada de registro>	Genera una entrada en el registro de la regla. Al seleccionar este tipo de acción, el Asistente **Gestionar regla** le solicita que especifique un texto para la entrada del registro. Cuando se especifica el texto del registro, se puede insertar variables, tales como **$DeviceName$**, **$EventName$**, en el mensaje de registro. **Ninguna acción de parada obligatoria**: Este tipo de acción no requiere una acción de detención. Puede especificar acciones de detención opcional que se deben realizar en cualquiera de un evento o después de un período de tiempo.
Iniciar plug-in en <dispositivos>	Inicia uno o más plug-ins. Cuando selecciona este tipo de acción, el Asistente **Gestionar regla** le solicita que seleccione los complementos necesarios y en qué dispositivos iniciar los complementos. Este tipo de acción requiere que haya al menos uno o más plug-ins instalados en el sistema. **Ninguna acción de parada obligatoria**: Este tipo de acción no requiere una acción de detención. Puede especificar acciones de detención opcional que se deben realizar en cualquiera de un evento o después de un período de tiempo.

Acción	Descripción
Detener plug-in en <dispositivos>	Detiene uno o más plug-ins. Cuando selecciona este tipo de acción, el asistente **Gestionar regla** le solicita que seleccione los complementos necesarios y en qué dispositivos para detener los complementos. Este tipo de acción requiere que haya al menos uno o más plug-ins instalados en el sistema. **Ninguna acción de parada obligatoria**: Este tipo de acción no requiere una acción de detención. Puede especificar acciones de detención opcional que se deben realizar en cualquiera de un evento o después de un período de tiempo.
Aplicar nueva configuración en <dispositivos>	Cambia la configuración del dispositivo en uno o más dispositivos. Al seleccionar este tipo de acción, el asistente **Gestionar regla** le pide que seleccione los dispositivos pertinentes, y se puede definir los ajustes pertinentes en los dispositivos que se han especificado. Si se define la configuración de más de un dispositivo, sólo se puede cambiar la configuración que están disponibles para todos los dispositivos especificados. **Ejemplo**: Se especifica que la acción debe estar vinculado a dispositivos 1 y 2. Dispositivo El dispositivo 1 tiene la configuración A, B y C, y el dispositivo 2 tiene la configuración B, C y D. En este caso, sólo se puede cambiar la configuración que está disponible para ambos dispositivos, a saber settings B y C. **Ninguna acción de parada obligatoria**: Este tipo de acción no requiere una acción de detención. Puede especificar acciones de detención opcional que se deben realizar en cualquiera de un evento o después de un período de tiempo.
Ajustar Matrix a vista <dispositivos>	Hace que el vídeo de las cámaras seleccionadas aparecen en un equipo capaz de mostrar vídeo Matrix activada por ejemplo, un ordenador en el que ha instalado ya sea XProtect Smart Client o la aplicación Matrix Monitor. Al seleccionar este tipo de acción, asistente **Gestionar regla** le pedirá que seleccione un destinatario de Matrix, y uno o más dispositivos desde los cuales para mostrar vídeo en el receptor de Matrix seleccionada. Este tipo de acción le permite seleccionar sólo un único destinatario de Matrix a la vez. Si usted quiere hacer el vídeo de los dispositivos seleccionados aparecen en más de un destinatario de Matrix, se debe crear una regla para cada destinatario Matrix requerida o utilizar la función XProtect Smart Wall . Al hacer clic con el botón secundario en una regla de la lista **Reglas**, puede copiar y volver a utilizar el contenido de las reglas. De esta manera, se puede evitar tener que crear reglas casi idénticas a partir de cero. Como parte de la configuración en los propios destinatarios Matrix, los usuarios deben especificar el número de puerto y la contraseña necesarios para el Matrix comunicación. Asegúrese de que los usuarios tienen acceso a esta información. Los usuarios deben normalmente también definir las direcciones IP de los hosts permitidos a partir del cual se acepta comandos con respecto a la pantalla de Matrix de video por alarma. En ese caso, los usuarios también deben conocer la dirección IP del servidor de gestión, o cualquier router o firewall utilizado.
Enviar captura SNMP	Genera un pequeño mensaje, que registra los eventos en los dispositivos seleccionados. El texto de trampas SNMP es generada automáticamente y no se puede modificar para requisitos particulares. Puede contener el tipo de fuente y el nombre del dispositivo en el que se produjo el evento.

Acción	Descripción
	Ninguna acción de parada obligatoria: Este tipo de acción no requiere una acción de detención. Puede especificar acciones de detención opcional que se deben realizar en cualquiera de un evento o después de un período de tiempo.
Recuperar y almacenar grabaciones a distancia desde <dispositivos>.	Recupera y almacena grabaciones remotas desde dispositivos seleccionados (que la grabación borde de soporte) en un período determinado antes y después del evento desencadenante. Tenga en cuenta que esta regla es independiente de ajuste **recuperación automática de grabaciones remotas cuando la conexión se restablece**. **Ninguna acción de parada obligatoria**: Este tipo de acción no requiere una acción de detención. Puede especificar acciones de detención opcional que se deben realizar en cualquiera de un evento o después de un período de tiempo.
Recuperar y almacenar grabaciones a distancia entre <hora de inicio y fin> desde <dispositivos>.	Recupera y almacena grabaciones remotas en un plazo determinado a partir dispositivos seleccionados (que la grabación borde de apoyo). Tenga en cuenta que esta regla es independiente de ajuste **recuperación automática de grabaciones remotas cuando la conexión se restablece**. **Ninguna acción de parada obligatoria**: Este tipo de acción no requiere una acción de detención. Puede especificar acciones de detención opcional que se deben realizar en cualquiera de un evento o después de un período de tiempo.
Guarda la imagen adjunta	Asegura que cuando una imagen obtenida desde el evento recibido Imágenes (enviada por correo electrónico SMTP desde una cámara), se guarda para uso futuro. En el futuro, otros eventos pueden desencadenar posiblemente también esta acción. **Ninguna acción de parada obligatoria**: Este tipo de acción no requiere una acción de detención. Puede especificar acciones de detención opcional que se deben realizar en cualquiera de un evento o después de un período de tiempo.
Activar archivo en <archivos>	Empiece a archivar en uno o más archivos. Al seleccionar este tipo de acción, asistente **Gestionar regla** le pide que seleccione los archivos pertinentes. **Ninguna acción de parada obligatoria**: Este tipo de acción no requiere una acción de detención. Puede especificar acciones de detención opcional que se deben realizar en cualquiera de un evento o después de un período de tiempo.
En el <sitio>, active el <evento definido por el usuario>	Relevante sobre todo dentro de Milestone Federated Architecture, pero también se puede usar esta configuración en un solo sitio. Use la regla para desencadenar un evento definido por el usuario en un sitio, normalmente un sitio remoto dentro de una jerarquía federada. **Ninguna acción de parada obligatoria**: Este tipo de acción no requiere una acción de detención. Puede especificar acciones de detención opcional que se deben realizar en cualquiera de un evento o después de un período de tiempo.

Acción	Descripción
Mostrar <access request notification>	Le permite acceder a notificaciones de solicitud de pop-up en la pantalla XProtect Smart Client cuando se cumplen los criterios para los eventos de activación. Milestone recomienda el uso de eventos de control de acceso eventos que activan esta acción, ya petición de acceso notificaciones normalmente están configurados para operar sobre los comandos de control de acceso y cámaras afines. Este tipo de acción requiere que tenga al menos un control de acceso plug-in instalado en su sistema. **Ninguna acción de parada obligatoria**: Este tipo de acción no requiere una acción de detención. Puede especificar acciones de detención opcional que se deben realizar en cualquiera de un evento o después de un período de tiempo.
Conectar la <cámara> al <canal DLNA basado en reglas>	Las cámaras se asignan al canal DLNA basado en reglas en función de los eventos. Este tipo de acción requiere que tenga un servidor DLNA instalado en su sistema. **Ninguna acción de parada obligatoria**: Este tipo de acción no requiere una acción de detención. Puede especificar acciones de detención opcional que se deben realizar en cualquiera de un evento o después de un período de tiempo.
Borrar <cámara> del <canal DLNA basado en reglas>	Las cámaras se eliminan del canal DLNA basado en reglas en función de los eventos. Este tipo de acción requiere que tenga un servidor DLNA instalado en su sistema. **Ninguna acción de parada obligatoria**: Este tipo de acción no requiere una acción de detención. Puede especificar acciones de detención opcional que se deben realizar en cualquiera de un evento o después de un período de tiempo.
Borrar cámara actual del <canal DLNA basado en reglas>	La cámara con la secuencia activa se elimina del canal DLNA basado en reglas en función de los eventos. Este tipo de acción requiere que tenga un servidor DLNA instalado en su sistema. **Ninguna acción de parada obligatoria**: Este tipo de acción no requiere una acción de detención. Puede especificar acciones de detención opcional que se deben realizar en cualquiera de un evento o después de un período de tiempo.

Visión general Eventos

Cuando agrega una regla basada en eventos en el asistente **Gestionar regla** , puede seleccionar entre varios tipos de eventos diferentes. Para que usted pueda obtener una buena visión general, los eventos se pueden seleccionar se clasifican en grupos de acuerdo a si son:

Hardware:

Alguno de hardware es capaz de crear acontecimientos en sí, por ejemplo, para detectar el movimiento. Usted puede utilizar éstos como los acontecimientos, sino que debe configurarlos en el hardware antes de poder utilizarlos en el sistema. Sólo puede ser capaz de utilizar los eventos enumerados en algún hardware ya que no todos los tipos de cámaras pueden detectar alteraciones o cambios de temperatura.

Hardware - eventos configurables:

Eventos configurables de hardware son importados automáticamente a partir de los controladores de dispositivos. Esto significa que varían desde el hardware al hardware y no se documentan aquí. Los eventos configurables no se activan hasta que los haya agregado al sistema y los haya configurado en la pestaña **Evento**

para hardware. Algunos de los eventos configurables también requieren la configuración de la cámara (hardware) en sí.

Hardware - predefinidos eventos:

Evento	Descripción
Error de comunicación (hardware)	Se produce cuando se pierde una conexión con el hardware.
Comunicación iniciada (hardware)	Se produce cuando se establece correctamente la comunicación con el hardware.
Comunicación detenida (hardware)	Se produce cuando la comunicación con el hardware se ha detenido correctamente.

Dispositivos - eventos configurables:

Eventos configurables de los dispositivos se importan automáticamente desde los controladores de dispositivos. Esto significa que varían de un dispositivo a otro y no se documentan aquí. Eventos configurables no se activan hasta que haya añadido al sistema y les configurado en la pestaña **evento** en un dispositivo.

Dispositivos - eventos predefinidos:

Evento	Descripción
Referencia de marcador solicitada	Se produce cuando un marcador se realiza en modo directo o de reproducción de los clientes. Además, un requisito para utilizar el registro por defecto en la regla de marcador.
Error de comunicación (Dispositivo)	Se produce cuando se pierde una conexión a un dispositivo, o cuando se hace un intento de comunicarse con un dispositivo, y el intento no tiene éxito.
Comunicación iniciada (Dispositivo)	Se produce cuando se establece correctamente la comunicación con un dispositivo.
Comunicación detenida (Dispositivo)	Se produce cuando la comunicación con un dispositivo se ha detenido correctamente.
Bloqueo de evidencias cambiado	Se produce cuando un bloqueo de evidencia se cambia para dispositivos por un usuario cliente oa través del SDK MIP.
Evidencia bloqueada	Se produce cuando un bloqueo de evidencia se crea para dispositivos por un usuario cliente o mediante el SDK MIP.
Evidencia desbloqueada	Se produce cuando un bloqueo de pruebas se elimina para los dispositivos por un usuario cliente o mediante el MIP SDK.

Evento	Descripción
Desbordamiento de entrada iniciado	Desbordamiento Feed (desbordamiento de medios de comunicación) se produce cuando un servidor de grabación no puede procesar los datos recibidos tan pronto como se especifica en la configuración y por lo tanto se ve obligado a desechar algunas grabaciones. Si el servidor está sano, el desbordamiento de alimentación por lo general ocurre a causa de las escrituras en disco lentos. Puede resolver este ya sea mediante la reducción de la cantidad de datos por escrito, o mejorando el rendimiento del sistema de almacenamiento. Reducir la cantidad de datos escritos mediante la reducción de las tasas de imagen, resolución o calidad de imagen de las cámaras, pero éstos podrían degradar la calidad de la grabación. Si no está interesado en que, en lugar de mejorar el rendimiento de su sistema de almacenamiento mediante la instalación de unidades adicionales para compartir la carga o mediante la instalación de discos o controladores más rápidos. Puede utilizar este evento para desencadenar acciones que le ayuda a evitar el problema, por ejemplo, para bajar la velocidad de grabación.
Desbordamiento de entrada detenido	Se produce cuando el Desbordamiento de entrada (ver descripción del evento **Desbordamiento de entrada Inicio**) termina.
Entrada de cliente en directo solicitada	Se produce cuando los usuarios de clientes solicitan una transmisión en vivo desde un dispositivo. El evento se produce a petición incluso si la solicitud del usuario del cliente más adelante resulta ser sin éxito, por ejemplo porque el usuario cliente no tiene los derechos necesarios para ver en directo solicitado o porque la alimentación es por alguna razón se detuvo.
Entrada de cliente en directo terminada	Se produce cuando los usuarios del cliente ya no solicitan una transmisión en vivo desde un dispositivo.
Grabación manual iniciada	Se produce cuando un usuario cliente inicia una sesión de grabación para una cámara. El evento se desencadena incluso si el dispositivo ya está grabando mediante acciones de reglas.
Grabación manual detenida	Se produce cuando un usuario cliente deja una sesión de grabación para una cámara. Si el sistema de reglas también ha iniciado una sesión de grabación continúa grabando incluso después de detener la grabación manual.
Referencia de datos marcados solicitada	Se produce cuando se realiza un bloqueo de evidencia en el modo de reproducción en los clientes o mediante el MIP SDK. Se crea un evento que se puede utilizar en las reglas.

Evento	Descripción
Movimiento iniciado	Se produce cuando el sistema detecta movimiento en el vídeo recibido desde cámaras. Este tipo del evento requiere que la detección de movimiento del sistema esté habilitada para las cámaras a las que se vincula el evento. Además de la detección de movimiento del sistema, algunas cámaras pueden detectar el movimiento y activar el evento **Comienzo del movimiento (HW)**, pero depende de la configuración del hardware de la cámara y del sistema. Ver **Hardware - eventos configurables** anteriormente.
Movimiento detenido	Se produce cuando el movimiento ya no se detecta en el vídeo recibido. Véase también la descripción del evento **Movimiento iniciado**. Este tipo Del evento requiere que la detección de movimiento del sistema esté habilitada para las cámaras a las que se vincula el evento. Además de la detección de movimiento del sistema, algunas cámaras pueden detectar movimiento a sí mismos y desencadenar el movimiento parado (HW) de eventos, pero depende de la configuración del hardware de la cámara y en el sistema. Ver **Hardware - eventos configurables** anteriormente.
Salida activada	Se produce cuando se activa un puerto de salida externo en un dispositivo. Este tipo de evento requiere que por lo menos un dispositivo en su sistema es compatible con puertos de salida.
Salida cambiada	Se produce cuando se cambia el estado de un puerto de salida externa en un dispositivo. Este tipo de evento requiere que por lo menos un dispositivo en su sistema es compatible con puertos de salida.
Salida desactivada	Se produce cuando se desactiva un puerto de salida externa en un dispositivo. Este tipo de evento requiere que por lo menos un dispositivo en su sistema es compatible con puertos de salida.
Sesión manual de PTZ iniciada	Se produce cuando se inicia una sesión de PTZ de accionamiento manual (en oposición a una sesión de PTZ basado en patrullaje programado o automáticamente provocada por un evento) en una cámara. Este tipo de evento requiere que las cámaras a la que está vinculado el evento son las cámaras PTZ.
Sesión manual de PTZ detenida	Se produce cuando una sesión de PTZ de accionamiento manual (en oposición a una sesión de PTZ basado en patrullaje programado o automáticamente provocada por un evento) se detiene en una cámara. Este tipo de evento requiere que las cámaras a la que está vinculado el evento son las cámaras PTZ.

Evento	Descripción
Grabación iniciada	Se produce cada vez que se inicia la grabación. Hay un evento separado para comenzó la grabación manual.
Grabación detenida	Se produce cada vez que se detiene la grabación. Hay un evento separado para la grabación manual detuvo.
Configuración cambiada	Se produce cuando configuración de un dispositivo se cambian con éxito.
Error de cambio de configuración	Se produce cuando se hace un intento para cambiar la configuración en un dispositivo, y el intento no tiene éxito.

Los eventos externos - eventos predefinidos:

Evento	Descripción
Solicitar la reproducción de mensajes de audio	Se activa cuando se solicitan mensajes de audio de reproducción a través del MIP SDK (kit de desarrollo de software). A través del MIP SDK, un proveedor externo puede desarrollar plug-ins personalizados (por ejemplo, integración con sistemas de control de acceso externos o similares) para su sistema.
Solicitar inicio de grabación	Activado cuando se solicitan las grabaciones iniciales mediante el Kit de desarrollo de software MIP (SDK). A través del MIP SDK, un proveedor externo puede desarrollar plug-ins personalizados (por ejemplo, integración con sistemas de control de acceso externos o similares) para su sistema.
Solicitar parada de grabación	Activado cuando se solicitan grabaciones de detención a través del MIP SDK. A través del MIP SDK, un proveedor externo puede desarrollar plug-ins personalizados (por ejemplo, integración con sistemas de control de acceso externos o similares) para su sistema.

Los eventos externos - eventos genéricos:

Eventos genéricos le permiten activar acciones en el sistema mediante el envío de cadenas simples a través de la red IP para el sistema. El propósito de eventos genéricos es permitir que el mayor número de fuentes externas como sea posible para interactuar con el sistema.

Los eventos externos - eventos definidos por el usuario:

Una serie de eventos a medida para adaptarse a su sistema también puede ser seleccionable. Puede utilizar este tipo de eventos definidos por el usuario para:

- Haciendo posible que los usuarios del cliente para activar manualmente los eventos durante la visualización de vídeo en directo en los clientes.

- Innumerables otros fines. Por ejemplo, puede crear eventos definidos por el usuario que se producen si un determinado tipo de datos se reciben desde un dispositivo.

  Consulte Eventos definidos por el usuario (explicado) (ver "Eventos definidos por el usuario (explicados)" en la página 218) para obtener más información.

Grabación de servidores:

Evento	Descripción
Archivo disponible	Se produce cuando un archivo de un servidor de grabación vuelve a estar disponible después de haber estado disponible (ver **Archivo No Disponible**).
Archivo no disponible	Se produce cuando un archivo de un servidor de grabación no está disponible, por ejemplo, si se pierde la conexión a un archivo ubicado en una unidad de red. En tales casos, no se puede archivar las grabaciones. Puede utilizar el evento para, por ejemplo, activar una alarma o un perfil de notificación para que una notificación por correo electrónico se envía automáticamente a las personas pertinentes en su organización.
No acabado Archivo	Se produce cuando un archivo de un servidor de grabación no ha terminado con la última ronda de archivado cuando la próxima está programada para comenzar.
Base de datos eliminando grabaciones antes de ajustar el tamaño de retención	Se produce cuando se alcanza el límite de tiempo de retención antes del límite de tamaño de la base de datos.
Base de datos eliminando grabaciones antes de ajustar el tiempo de retención	Se produce cuando se alcanza el límite de tamaño de la base de datos antes del límite de tiempo de retención.
Disco de base de datos lleno - Autoarchivado	Se produce cuando un disco de base de datos está lleno. Un disco de base de datos se considera completa cuando hay menos de 5 GB de espacio se deja en el disco: Los datos más antiguos en una base de datos siempre han archivado automáticamente (o eliminado si no se define ningún archivo siguiente) cuando menos de 5 GB de espacio está libre.
Disco de base de datos lleno - Eliminando	Se produce cuando un disco de base de datos está lleno y menos de 1 GB de espacio libre. Los datos se eliminan incluso si se define un archivo siguiente. Una base de datos siempre requiere de 250 MB de espacio libre. Si se alcanza este límite (si los datos no se eliminan suficientemente rápido), no hay más datos se escriben en la base de datos hasta que haya suficiente espacio ha sido liberado. El tamaño máximo real de su base de datos es la cantidad de gigabytes que especifica, menos 5 GB.
Base de datos llena: autoarchivado	Se produce cuando un archivo de un servidor de grabación está lleno y necesita auto-archivo en un archivo en el almacenamiento.

Evento	Descripción
Reparación de base de datos	Se produce si una base de datos resulta dañada, en cuyo caso el sistema intenta automáticamente dos métodos de reparación de bases de datos diferentes: una reparación rápida y una reparación a fondo.
Área de almacenamiento disponible	Se produce cuando un dispositivo de almacenamiento para un servidor de grabación vuelve a estar disponible después de haber estado disponible (véase el **almacenamiento de base de datos no disponible**). Puede, por ejemplo, utilizar el evento para iniciar la grabación si ha sido detenido por un **base de datos de almacenamiento disponible** evento.
Almacenamiento de base de datos no disponible	Se produce cuando un dispositivo de almacenamiento para un servidor de grabación no está disponible, por ejemplo, si se pierde la conexión a un compartimiento situado en una unidad de red. En tales casos, no se puede archivar las grabaciones. Puede utilizar el evento para, por ejemplo, detener la grabación, activar una alarma o un perfil de notificación para una notificación por correo electrónico se envía automáticamente a las personas pertinentes en su organización.
Failover iniciado	Se produce cuando un servidor de grabación failover se hace cargo de un servidor de grabación. Ver Servidores de grabación failover (explicado) (ver "Servidores de grabación con conmutación por error (explicado)" en la página 101).
Failover detenido	Se produce cuando un servidor de grabación vuelva a estar disponible, y puede tomar el relevo de un servidor de grabación failover.

Eventos del monitor del sistema

Los eventos del supervisor del sistema se desencadenan por valores umbrales excedidos configurados en el nodo **Umbrales del monitor del sistema** (ver "**Umbrales del monitor del sistema (explicados)**" en la página 265).

Esta funcionalidad requiere que el servicio Milestone XProtect Data Collector Server se esté ejecutando.

Monitor del sistema - Servidor:

Evento	Descripción
Uso de CPU crítico	Se produce cuando el uso de la CPU excede el umbral crítico de la CPU.
Uso de CPU normal	Se produce cuando el uso de la CPU cae por debajo del umbral de la CPU de advertencia.
Aviso de uso de CPU	Ocurre cuando el uso de la CPU excede el umbral de la CPU de advertencia o cae por debajo del umbral crítico de la CPU.

Evento	Descripción
Uso de memoria crítico	Se produce cuando el uso de memoria excede el umbral de memoria crítica.
Uso de memoria normal	Se produce cuando el uso de memoria cae por debajo del umbral de memoria de advertencia.
Aviso de uso de memoria	Se produce cuando el uso de la memoria excede el umbral de la memoria de advertencia o cae por debajo del umbral de uso de la memoria crítica.
Decodificación de NVIDIA crucial	Se produce cuando el uso de decodificación NVIDIA excede el umbral de descodificación NVIDIA crítico.
Decodificación de NVIDIA normal	Se produce cuando el uso de decodificación de NVIDIA cae por debajo del umbral de advertencia de NVIDIA.
Aviso de la decodificación de NVIDIA	Se produce cuando el uso de decodificación de NVIDIA excede el umbral de descodificación NVIDIA de advertencia o cae por debajo del umbral de descodificación NVIDIA crítico.
Memoria de NVIDIA crucial	Se produce cuando el uso de la memoria NVIDIA excede el umbral de memoria NVIDIA crítico.
Memoria de NVIDIA normal	Se produce cuando el uso de la memoria NVIDIA cae por debajo del umbral de advertencia de memoria NVIDIA.
Aviso de la memoria de NVIDIA	Se produce cuando el uso de la memoria NVIDIA excede el umbral de memoria NVIDIA de advertencia o cae por debajo del umbral de memoria NVIDIA crítico.
Procesamiento de NVIDIA crucial	Se produce cuando el uso de la representación de NVIDIA excede el umbral crítico de reproducción de NVIDIA.
Procesamiento de NVDIA normal	Se produce cuando el uso de la representación de NVIDIA cae por debajo del umbral de advertencia de NVIDIA.
Aviso del procesamiento de NVIDIA	Se produce cuando el uso de la representación de NVIDIA excede el umbral de advertencia de NVIDIA o cae por debajo del umbral crítico de reproducción de NVIDIA.
Servicios disponibles crítico	Se produce cuando un servicio de servidor deja de ejecutarse. No hay valores de umbral para este evento.
Servicios disponibles normal	Se produce cuando un estado de servicio del servidor cambia a ejecutarse. No hay valores de umbral para este evento.

Monitor del sistema - Cámara:

Evento	Descripción
FPS en directo crítico	Se produce cuando la velocidad de FPS en vivo cae por debajo del umbral crítico de FPS en vivo.

Evento	Descripción
FPS en directo normal	Se produce cuando la velocidad de FPS en vivo excede el umbral de FPS en vivo de advertencia.
Aviso de FPS en directo	Ocurre cuando la tasa de FPS en vivo cae por debajo del umbral de FPS en vivo de advertencia o excede el umbral crítico de FPS en vivo.
Grabando FPS crítico	Se produce cuando la velocidad de grabación de FPS cae por debajo del umbral de grabación crítica de FPS.
Grabando FPS normal	Se produce cuando la velocidad de grabación de FPS excede el umbral de grabación de advertencia de FPS.
Aviso de grabando FPS	Se produce cuando la velocidad de grabación de FPS cae por debajo del umbral de grabación de advertencia de FPS o excede el umbral de grabación crítica de FPS.
Espacio utilizado crítico	Se produce cuando el almacenamiento utilizado para las grabaciones de una cámara específica supera el umbral de espacio utilizado crítico.
Espacio utilizado normal	Se produce cuando el almacenamiento utilizado para las grabaciones de una cámara específica cae por debajo del umbral de espacio utilizado de advertencia.
Aviso de espacio utilizado	Se produce cuando el almacenamiento utilizado para las grabaciones de una cámara específica excede el umbral de espacio utilizado de advertencia o cae por debajo del umbral de espacio utilizado crítico.

Monitor del sistema - Disco:

Evento	Descripción
Espacio libre crítico	Se produce cuando el uso de espacio en disco excede el umbral crítico de espacio libre.
Espacio libre normal	Se produce cuando el uso de espacio en disco cae por debajo del umbral de espacio libre de advertencia.
Aviso de espacio libre	Se produce cuando el uso de espacio en disco excede el umbral de espacio libre de advertencia o cae por debajo del umbral de espacio libre crítico.

Monitor del sistema - Almacenamiento:

Evento	Descripción
Periodo de retención crítico	Se produce cuando el sistema predice que el almacenamiento se llenará más rápido que el valor límite del tiempo de retención crítico. Por ejemplo, cuando los datos de las transmisiones de video están llenando el almacenamiento más rápido de lo esperado.

Evento	Descripción
Periodo de retención normal	Se produce cuando el sistema predice que el almacenamiento se llenará más lento que el valor del umbral de tiempo de retención de advertencia. Por ejemplo, cuando los datos de las transmisiones de video llenan el almacenamiento a la velocidad esperada.
Aviso de periodo de retención	Se produce cuando el sistema predice que el almacenamiento se llenará más rápido que el valor del umbral de tiempo de retención de advertencia o más lento que el valor del umbral del tiempo de retención crítico. Por ejemplo, cuando los datos de las transmisiones de video están llenando el almacenamiento más rápido de lo esperado debido a que las cámaras configuradas para grabar en movimiento detectan más movimiento.

Otro:

Evento	Descripción
Error en la activación automática de licencia	Se produce cuando falla la activación automática de la licencia en línea. No hay valores de umbrales para este evento.

Eventos de productos complementarios e integraciones:

Eventos de productos e integraciones add-on se pueden utilizar en el sistema de reglas, por ejemplo:

- Eventos analiticos también se pueden utilizar en el sistema de reglas.

Reglas

Reglas (explicadas)

Las reglas especifican las acciones a llevar a cabo en condiciones particulares. Ejemplo: Cuando se detecta movimiento (condición), una cámara debe empezar a grabar (acción).

Los siguientes son **ejemplos** de lo que puede hacer con las normas:

- Inicio y detención de la grabación
- Ajuste de velocidad de fotogramas en directo no predeterminada
- Establecer velocidad de grabación no es el predeterminado
- Inicio y parada de patrulla PTZ
- Pausa y reanudación de patrulla PTZ
- Mover las cámaras PTZ a posiciones específicas
- Ajuste de salida en estado activado/desactivado

- Enviar notificaciones por correo electrónico
- Generar entradas de registro
- Generar eventos
- Aplicar nuevas configuraciones de dispositivo, por ejemplo una resolución diferente en una cámara
- Hacer que el vídeo en los receptores de la Matrix
- Iniciar y detener los plug-ins
- Iniciar y detener los fotogramas desde el dispositivo

Detención de un dispositivo significa que el vídeo ya no se transfiere desde el dispositivo al sistema, en cuyo caso no se puede ver vídeo en directo ni grabar video. Por el contrario, un dispositivo en el que haya detenido la alimentación todavía puede comunicarse con el servidor de grabación, y se puede empezar la alimentación del dispositivo de forma automática a través de una norma, a diferencia de cuando el dispositivo está desactivado manualmente en el Management Client.

Importante: Algunos de los contenidos de reglas puede requerir que ciertas funciones están habilitadas para los dispositivos pertinentes. Por ejemplo, una regla que especifica que una cámara debe grabar no funciona como está previsto si la grabación no está habilitada para la cámara correspondiente. Antes de crear una regla, Milestone recomienda comprobar que los dispositivos implicados pueden funcionar según lo previsto.

Reglas por defecto (explicadas)

Su sistema incluye varias reglas predeterminadas que puede utilizar para las funciones básicas sin configurar nada.Puede desactivar o modificar las reglas predeterminadas como sea necesario. Si modifica o desactivar las reglas predeterminadas, el sistema puede no funcionar tan deseado ni garantiza que los canales de vídeo o alimentaciones de audio se introducen automáticamente en el sistema.

Regla por defecto	Descripción
Ir a predefinido cuando se hace PTZ	Asegura que las cámaras PTZ van a sus respectivas posiciones predefinidas por defecto después de que los haya operado manualmente. Esta regla no está habilitada por defecto. Aun cuando se ha activado la regla, debe haber definido las posiciones fijado de manera predeterminada para las cámaras PTZ pertinentes a fin de que la regla funcione. Esto se hace en la pestaña **Ajustes preestablecidos**.
Reproducir audio a petición	Asegura que el video se grabe automáticamente cuando se produce una petición externa. La solicitud está siempre activada por un sistema de integración de forma externa con el sistema, y el Estado es utilizado principalmente por los integradores de sistemas externos o plug-ins.

Regla por defecto	Descripción
Grabar en Añadir a favoritos	Asegura que el vídeo se graba de forma automática cuando un operario coloca un marcador en XProtect Smart Client. Esto está previsto que haya activado la grabación de las cámaras correspondientes. La grabación está activada por defecto. El tiempo de grabación por defecto para esta regla es de tres segundos antes de que el marcador se establece y 30 segundos después de que el marcador se establece. Puede editar los tiempos de grabación por defecto en la regla. Tenga en cuenta que el pre-buffer que se establece en la ficha de registro debe ser igual o mayor que el tiempo de pre-grabación.
Grabar en Movimiento	Asegura que siempre y cuando se detecta movimiento en el vídeo de las cámaras, se graba el vídeo, la grabación siempre está habilitada para las cámaras pertinentes. La grabación está activada de forma predeterminada. Si bien la regla por defecto especifica grabación basada en un movimiento detectado, no garantiza que el sistema graba vídeo, ya que puede tener la grabación con discapacidad cámaras individuales para una o más cámaras. Aun cuando se ha activado la grabación, recuerde que la calidad de las grabaciones puede verse afectada por los ajustes de grabación de la cámara individual.
Registro, previa petición	Asegura que el vídeo se graba automáticamente cuando se produce una petición externa, la grabación siempre está habilitada para las cámaras pertinentes. La grabación está activada por defecto. La solicitud está siempre activada por un sistema de integración de forma externa con el sistema, y el Estado es utilizado principalmente por los integradores de sistemas externos o plug-ins.
Comience Audio RSS	Asegura que el audio se alimenta de todos los micrófonos y altavoces conectados son alimentados automáticamente al sistema. Si bien la regla predeterminada permite el acceso a los micrófonos y altavoces conectados " de audio se alimenta inmediatamente después de la instalación del sistema, que no garantiza que el audio se graba, ya que debe especificar la configuración de grabación por separado.
Comience RSS	Asegura que los canales de vídeo de todas las cámaras conectadas se alimentan automáticamente al sistema. Si bien la regla predeterminada permite el acceso a las cámaras conectadas alimenta el vídeo inmediatamente después de la instalación del sistema, que no garantiza que el vídeo se graba, como cámaras de 'ajustes de grabación deben especificarse por separado.
Metadatos inicio RSS	Asegura que los datos se alimentan de todas las cámaras conectadas se alimentan automáticamente al sistema. Si bien la regla predeterminada permite el acceso a las cámaras conectadas 'fuentes de datos inmediatamente después de la instalación del sistema, esto no garantiza que los datos se registran, como cámaras de' ajustes de grabación deben especificarse por separado.

Regla por defecto	Descripción
Mostrar notificación de solicitud de acceso	Se asegura de que todos los eventos de control de acceso categorizados como "Solicitud de acceso ', daría lugar a una notificación de solicitud de acceso para que aparezca en el XProtect Smart Client, a menos que la función de notificación está desactivada en el perfil de Smart Client.

Volver a crear reglas predeterminadas

Si elimina accidentalmente cualquiera de las reglas predeterminadas, puede volver a ellos escribiendo el siguiente contenido:

Regla por defecto	Texto para escribir
Ir a predefinido cuando se hace PTZ	Realizar una acción en PTZ Manual de sesión detenida de todas las cámaras Pasar de inmediato al fijado de manera predeterminada en el dispositivo en el que se produjo evento
Reproducir audio a petición	Realizar una acción en Solicitar Reproducir Mensaje de Audio desde External Reproducir mensaje de mensaje de audio a partir de metadatos en los dispositivos de metadatos con prioridad 1
Grabar en Añadir a favoritos	Realizar una acción en Favorito referencia solicitada de todas las cámaras, todos los micrófonos, todos los altavoces empiezan a grabar tres segundos antes en el dispositivo en el que se produjo evento Realizar la acción 30 segundos después de la parada de la grabación inmediatamente
Grabar en Movimiento	Realizar una acción en movimiento de introducción de todas las cámaras empezar a grabar tres segundos antes de que el dispositivo en el que se produjo evento Realizar la acción parada en movimiento parado de todas las cámaras dejan de grabar tres segundos después de
Registro, previa petición	Realizar una acción sobre de petición de inicio de grabación de externo empieza a grabar inmediatamente en los dispositivos de metadatos Realizar la acción de parada a petición Detener grabación en la grabación Parada externa de inmediato
Comience Audio RSS	Realizar una acción en un intervalo de tiempo de inicio de alimentación siempre en todos los micrófonos, todos los altavoces Realizar una acción cuando termina el intervalo de tiempo de alimentación de terminación inmediatamente
Comience RSS	Realizar una acción en un intervalo de tiempo de inicio de alimentación siempre en todas las cámaras Realizar una acción cuando termina el intervalo de tiempo de alimentación de terminación inmediatamente

Regla por defecto	Texto para escribir
Metadatos inicio RSS	Realizar una acción en un intervalo de tiempo comienza siempre se alimentan de Todos los metadatos Realizar una acción cuando termina el intervalo de tiempo de alimentación de terminación inmediatamente
Mostrar notificación de solicitud de acceso	Realizar una acción en la solicitud de acceso (Categorías de control de acceso) de los sistemas [+unidades] Mostrar notificación de solicitud de acceso integrado

Complejidad de la regla (explicada)

El número exacto de opciones depende del tipo de regla que desee crear y del número de dispositivos disponibles en su sistema. Las reglas proporcionan un alto grado de flexibilidad: puede combinar condiciones evento y el tiempo, especificar varias acciones en una sola regla, y muy a menudo crear reglas relativas a varios o todos los dispositivos en el sistema.

Usted puede hacer sus reglas tan simple o compleja como se desee. Por ejemplo, puede crear reglas basadas en el tiempo muy simples:

Ejemplo	Explicación
Regla de la base del tiempo muy simple	Los lunes entre las 08. 30 y las 11. 30 (condición de tiempo), la cámara 1 y 2 de la cámara debe empezar a grabar (acción) cuando comience el período de tiempo y detener la grabación (detener la acción) cuando el período de tiempo.
Regla basada en eventos muy simple	Cuando se detecta movimiento (condición de evento) en la Cámara 1, Cámara 1 debería empezar a grabar (acción) de inmediato, y luego se detiene la grabación (la acción de parada) después de 10 segundos. Incluso si una regla basada en eventos es activada por un evento en un dispositivo, se puede especificar que las acciones deben llevarse a cabo en uno o más dispositivos.
Regla que implica varios dispositivos	Cuando se detecta movimiento (condición de evento) en la Cámara 1, Cámara 2 debería empezar a grabar (acción) de inmediato, y la sirena conectada a la salida 3 debe sonar (acción) inmediatamente. Luego, al cabo de 60 segundos, la cámara 2 se debe detener la grabación (acción de detención), y la sirena conectada a la salida 3 debe dejar de sonar (acción de detención).
Regla Combinando Tiempo, Eventos y Dispositivos	Cuando se detecta movimiento (condición de evento) en la cámara 1, y el día de la semana es el sábado o el domingo (condición de tiempo), la cámara 1 y cámara 2 debe empezar a grabar (acción) de inmediato, y una notificación debe ser enviada a la gerente de seguridad (acción). Entonces, después de 5 segundos de movimiento ya no se detectan en la cámara 1 o 2 de la cámara, las 2 cámaras deben detener la grabación (acción de detención).

Dependiendo de las necesidades de su organización, a menudo es una buena idea para crear muchas reglas simples en lugar de unas cuantas reglas complejas. Incluso si esto significa que tiene más reglas en el sistema, que proporciona una manera fácil de mantener una visión general de lo que sus reglas hacen. Mantener sus reglas simples también significa que usted tiene mucha más flexibilidad a la hora de desactivación / activación

elementos de regla individuales. Con reglas simples, puede desactivar / activar las reglas completas cuando sea necesario.

Reglas de validación (explicadas)

Puede validar el contenido de una norma individual o todas las reglas de una sola vez. Al crear una regla, el asistente de administración **Gestionar regla** garantiza que todos los elementos de la regla tengan sentido. Cuando una norma existe desde hace algún tiempo, uno o más de los elementos de la regla pueden haber sido afectados por la otra configuración, y el Estado ya no puede trabajar. Por ejemplo, si una regla se activa por un perfil determinado momento, la regla no funciona si ha eliminado ese perfil temporal o si ya no tiene permisos para ello. Tales efectos no deseados de configuración pueden ser difícil mantener una visión de conjunto.

Validación de reglas le ayuda a mantener un registro de lo que se han visto afectadas reglas. La validación se lleva a cabo en función de cada regla y cada regla es validada por sí mismos. No se puede validar reglas uno contra el otro, por ejemplo con el fin de ver si una regla de conflictos con otra regla, ni siquiera si se utiliza la función de validar todos **Reglas**.

Tenga en cuenta que no puede validar si la configuración de requisitos fuera de la propia regla puede impedir que la regla funcione. Por ejemplo, una regla que especifica que la grabación debería tener lugar cuando el movimiento es detectado por una cámara en particular valida bien si los elementos de la norma en sí son correctos, incluso si la detección de movimiento, que está habilitada en un nivel de la cámara, no a través de reglas, no ha ha habilitado para la cámara correspondiente.

Valida una regla individual o todas las reglas de una sola vez haciendo clic con el botón secundario en la regla que desea validar y seleccione **Validar regla** o **Validar todas las reglas**. Un cuadro de diálogo le informa de si la norma (s) validado con éxito o no. Si ha escogido validado más de una regla y una o más reglas no tuvo éxito, el cuadro de diálogo enumera los nombres de las normas en cuestión.

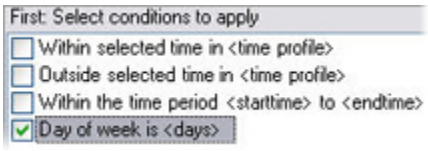
Añadir una regla

Cuando se crean reglas, el asistente **controla la regla** que sólo lista las opciones pertinentes.

Asegura que una norma no contiene elementos que faltan. Con base en el contenido de su regla, se sugiere automáticamente acciones de detención adecuado, eso es lo que debe tener lugar cuando la regla ya no se aplica, asegurando que no sin intención de crear una regla de nunca acabar.

1. Haga clic con el botón secundario en el objeto **Reglas** > **Añadir regla**. Esto abre el asistente **Administrar regla**. El asistente le guía a través de especificar el contenido de la regla.
2. Al especificar un nombre y una descripción de la nueva regla en campos **Nombre** y **Descripción** respectivamente.
3. Seleccione el tipo correspondiente de la condición de la regla: o bien una regla que lleva a cabo una o más acciones cuando se produce un evento en particular, o una regla que lleva a cabo una o más acciones cuando se introduce un período específico de tiempo.
4. Haga clic en **Siguiente** para ir al segundo paso del asistente. El segundo paso del asistente, definir otras condiciones de la regla.

5. Seleccione una o más condiciones, por ejemplo **Día de la semana es <día>**:



Dependiendo de las selecciones, editar la descripción de la regla en la parte inferior de la ventana del asistente:

Haga clic en los elementos subrayados en **negrita cursiva** para especificar su contenido exacto. Por ejemplo, haciendo clic en el enlace **días** en nuestro ejemplo le permite seleccionar uno o más días de la semana en los que se aplique la regla.

6. Una vez especificadas las condiciones exactas, haga clic en **Siguiente** para pasar al siguiente paso del asistente y seleccione las acciones que debe cubrir la regla. En función del contenido y la complejidad de la regla, puede que tenga que definir más medidas, como los eventos de detención y acciones de detención. Por ejemplo, si una regla especifica que un dispositivo debe ejecutar una acción concreta durante un intervalo de tiempo (por ejemplo, jueves entre las 08. 00 y las 10. 30), el asistente puede pedirle que especifique lo que debe suceder cuando termina ese intervalo de tiempo.

7. Su regla es activa de forma predeterminada una vez que lo haya creado si se cumplen las condiciones de la regla. Si no desea que la regla se active de inmediato, desactive la casilla de verificación **Activo**.

8. Haga clic en **Finalizar**.

Editar, copiar y cambiar el nombre de una regla

1. En el panel **general**, haga clic en la regla correspondiente.

2. Seleccione:

   Editar regla o **Copiar regla** o **Cambiar el nombre de la regla**. El asistente **Gestionar Regla** abre.

3. En el asistente, cambiar el nombre y / o cambiar la regla. Si ha seleccionado **Copiar regla**, se abre el asistente, mostrando una copia de la regla seleccionada.

4. Haga clic en **Finalizar**.

Desactivar y activar una regla

Su sistema se aplica una regla tan pronto como se aplican condiciones de la regla que significa que es activo. Si no desea que una norma no se activa, puede desactivar la regla. Al desactivar la regla, el sistema no se aplica la regla, incluso si se aplican condiciones de la regla. Se puede activar fácilmente una regla desactivada después.

Desactivación de una regla

1. En el panel **general**, seleccione la regla.

2. Desactive la casilla de verificación **Activo** en panel **Propiedades**.

3. Haga clic en **Guardar** en la barra de herramientas.

4. Un icono con una X roja indica que la regla se desactiva en la lista **Reglas**:

La activación de una regla

Cuando se desea activar nuevamente la regla, seleccione la regla, seleccione la casilla de verificación **Activar**, y guardar la configuración.

Perfiles temporales

Perfiles de tiempo (explicados)

Funcionalidad disponible depende del sistema que está utilizando. Ver tabla de comparación de productos (en la página 24) para más información.

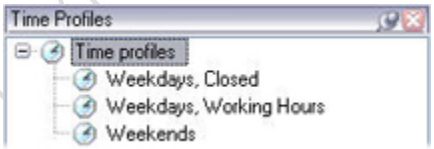
Perfiles temporales son periodos de tiempo definidos por el administrador. Puede utilizar perfiles temporales al crear reglas, por ejemplo, una regla que especifica que una determinada acción debe llevarse a cabo dentro de un cierto período de tiempo.

Perfiles temporales se asignan también a los cometidos, junto con los perfiles de Smart Client. De forma predeterminada, a todos los cometidos se les asigna el perfil temporal predeterminado **Siempre**. Esto significa que los miembros de cometidos con este perfil temporal predeterminado adjunto no tiene límites basados en el tiempo a sus derechos de usuario en el sistema. También puede asignar un perfil temporal alternativa a un cometido.

Perfiles temporales son muy flexibles: se puede basar en ellas uno o más períodos de tiempo individuales, en uno o más periodos recurrentes de tiempo, o una combinación de los tiempos individuales y recurrentes. Muchos usuarios pueden estar familiarizados con los conceptos de períodos de tiempo individuales y recurrentes de aplicaciones de calendario, como el de Microsoft® Outlook.

Perfiles temporales se aplican siempre en hora local. Esto significa que si el sistema ha de grabar servidores ubicados en diferentes zonas horarias, cualquier acción, por ejemplo, la grabación de las cámaras, asociado a perfiles temporales se llevan a cabo en el horario local de cada servidor de grabación. Ejemplo: Si usted tiene un perfil temporal que abarca el período comprendido entre 08.30 hasta 09.30, ningúnas acciones asociadas sobre un servidor de grabación colocada en Nueva York se lleva a cabo cuando es 08.30 a 09.30 en Nueva York, mientras que las mismas acciones en un servidor de grabación colocados en la hora local los Ángeles se lleva a cabo algunas horas más tarde, cuando la hora local es 08.30 a 09.30 en Los Ángeles.

Crea y administra perfiles temporales expandiendo **Reglas y eventos** > **Perfiles temporales**. Se abre una lista **Perfiles temporales** . Ejemplo solamente:



Para una alternativa a los perfiles de tiempo, vea Perfiles de tiempo de duración del día (explicado) (ver "Perfiles de longitud de día (explicado)" en la página 212).

Especificar un perfil temporal

1. En la lista **perfiles temporales**, haga clic con el botón secundario en **Perfiles temporales** > **Añadir perfil temporal**. Esto abre la ventana de **perfil temporal**.
2. En la ventana **Perfil temporal**, escriba un nombre para el nuevo perfil de tiempo en el campo **Nombre**. Opcionalmente, escriba una descripción del nuevo perfil temporal en el campo **Descripción**.
3. En ventana calendario **Perfil temporal**, seleccione **Vista de Día**, **vista de semana** o **vista mes**, a continuación, haga clic dentro del calendario y seleccione **Añadir tiempo individual** o **Añadir tiempo recurrencia**.
4. Cuando haya especificado los períodos de tiempo para su perfil de tiempo, haga clic en **OK** en la ventana **Perfiles temporales**. Su sistema agrega su nuevo perfil temporal a la lista **Perfiles temporales**. Si en una etapa posterior que desea editar o eliminar el perfil temporal, lo hace de la lista **Perfiles temporales** también.

Añadir una sola vez

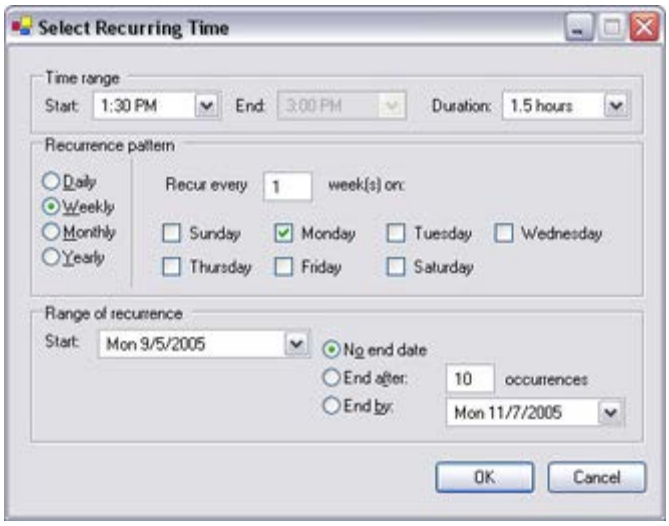
Al seleccionar **Añadir una única hora**, aparece la ventana de **Seleccionar tiempo**:

Formato de hora y la fecha pueden ser diferentes en su sistema.

1. En la ventana **Seleccione tiempo**, especifique **Hora de inicio** y **Hora de finalización**. Si el tiempo es para cubrir días enteros, seleccione el **Todo el día** cuadro.
2. **Haga clic en OK (aceptar)**.

Especificar un tiempo recurrente

Cuando se selecciona **Añadir hora periódica**, la ventana **Seleccionar hora periódica**:



1. En la ventana **Seleccionar hora**, especifique el intervalo de tiempo, patrón de repetición y la gama de repetición.
2. **Haga clic en OK (aceptar)**.

Un perfil temporal puede contener varios períodos de tiempo. Si desea que su perfil temporal para contener períodos de tiempo, añadir más veces individuales o recurrentes veces.

Editar un perfil temporal

1. En el **Descripción general** panel **Lista de perfiles temporales** lista, haga clic con el botón secundario en el perfil de tiempo correspondiente y seleccione **Editar perfil temporal**. Esto abre la ventana **Perfil temporal**.
2. Editar el perfil temporal según sea necesario. Si ha realizado cambios en el perfil temporal, haga clic en **OK** en la ventana **perfil temporal**. Se vuelve a la lista de **perfiles temporales**.

Nota: En la ventana **Información de perfil temporal**, puede editar el perfil temporal según sea necesario. Recuerde que un perfil temporal puede contener más de un período de tiempo, y que los períodos de tiempo puede ser recurrente. La visión general pequeña mes en la esquina superior derecha puede ayudarle a obtener una visión rápida de los períodos de tiempo cubiertos por el perfil temporal, ya que las fechas contienen tiempos especificados se destacan en negrita.

En este ejemplo, las fechas en negrita indican que ha especificado períodos de tiempo durante varios días, y que se ha especificado un tiempo recurrente los lunes.

Perfiles de longitud de día (explicado)

Cuando se coloca cámaras fuera, se debe a menudo bajar la resolución de la cámara, permitirá negro / blanco o cambiar otros ajustes cuando se hace de noche o cuando se pone la luz. Cuanto más al norte o al sur del

ecuador las cámaras se colocan, más el tiempo de amanecer y al atardecer varía durante el año. Esto hace que sea imposible el uso de perfiles normales de tiempo fijo para ajustar las configuraciones de la cámara según las condiciones de luz.

En tales situaciones, se pueden crear perfiles temporales la duración del día en lugar de definir la salida y la puesta del sol en un área geográfica determinada. A través de coordenadas GPS, el sistema calcula la hora del amanecer y el atardecer, incluso la incorporación de horario de verano en una base diaria. Como resultado, el perfil temporal sigue automáticamente los cambios anuales en la salida del sol / puesta del sol en el área seleccionada, asegurando que el modo permanezca activo sólo cuando sea necesario. Todos los horarios y las fechas se basan en el tiempo de los servidores de gestión y configuración de la fecha. También puede establecer un desplazamiento positivo o negativo (en minutos) para la puesta de sol (amanecer) y de final (puesta del sol). La compensación para el inicio y la hora de finalización puede ser igual o diferente.

Puede utilizar los perfiles de la longitud del día, tanto al crear reglas y cometidos.

Crear un perfil temporal de duración del día

1. Ampliar las **Reglas y Eventos** carpeta > **Perfiles Temporal**.
2. En la lista de **Perfiles Temporales**, haga clic **Perfiles Temporales**, y seleccione **Añadir perfil temporal de duración de día**.
3. En la ventana **Perfil temporal de duración de día**, complete la información necesaria. Para hacer frente a los períodos de transición entre claridad y oscuridad, se puede compensar la activación y desactivación del perfil. La hora y el nombre de meses se muestran en el idioma que se utiliza la configuración de idioma / regional de su equipo.
4. Para ver la ubicación de las coordenadas GPS introducidas en un mapa, haga clic en **Mostrar posición en el navegador**. Esto abre un navegador donde se puede ver la situación.
5. **Haga clic en OK (aceptar)**.

Día de las propiedades de perfil temporal de longitud

Establezca las siguientes propiedades para la duración del día perfil temporal:

Nombre	Descripción
Nombre	El nombre del perfil.
Descripción	Una descripción del perfil (opcional).
Coordenadas GPS	Coordenadas GPS que indica la ubicación física de la cámara (s) asignado al perfil.
Salida del sol de desplazamiento	Número de minutos (+/-) por el cual la activación del perfil se ve compensado por la salida del sol.
Sunset desplazamiento	Número de minutos (+/-) por el cual la desactivación del perfil se ve compensado por la puesta del sol.
Zona horaria	Zona de tiempo que indica la ubicación física de la cámara (s).

Perfiles de notificación

Perfiles de notificación (explicados)

Los perfiles de notificación le permiten configurar notificaciones por correo electrónico ya preparadas, las cuales se pueden activar de forma automática por regla general, por ejemplo, cuando se produce un evento en particular. Puede incluir imágenes fijas y clips de vídeo AVI en las notificaciones por correo electrónico.

El sistema no es compatible con TLS (Transport Layer Security) y su predecesor SSL (Secure Socket Layer). Si el remitente pertenece en un servidor que requiere TLS o SSL, notificaciones de correo electrónico no funcionan correctamente. Además, es posible que tenga que desactivar cualquier escáner de correo electrónico que podrían impedir que la aplicación envíe las notificaciones por correo electrónico.

Requisitos para crear perfiles de notificación

Antes de poder crear perfiles de notificación, debe especificar la configuración para el servidor de correo saliente SMTP para las notificaciones por correo electrónico.

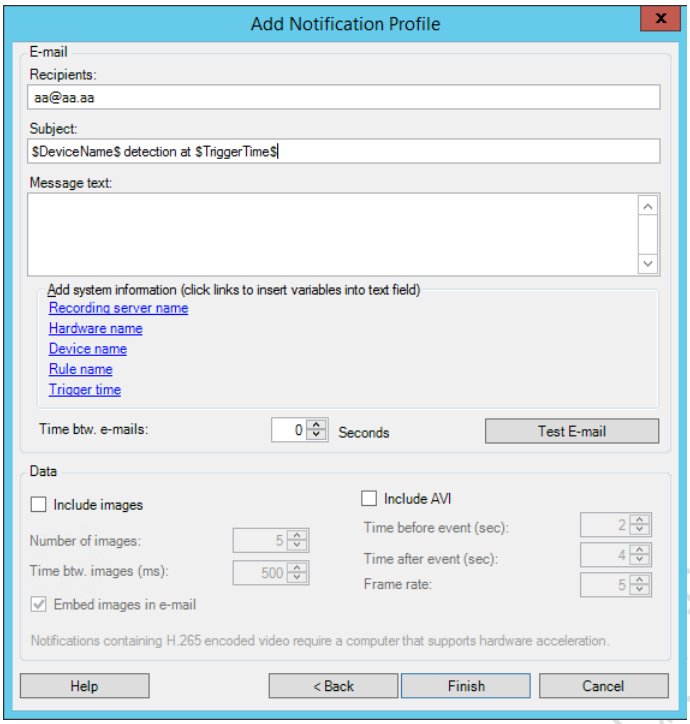
Si desea que las notificaciones de correo electrónico para poder incluir clips de película AVI, también debe especificar los ajustes de compresión a utilizar.

1. Ir a **Herramientas** > **Opciones**. Esto abre la ventana **Opciones**.
2. Especificar el **servidor de correo saliente SMTP** en la ficha **servidor Correo** y los ajustes de compresión en la pestaña **Generación AVI**.

Añadir los perfiles de notificación

1. Expandir **Reglas y eventos**, haga clic con el botón secundario del mouse en **Perfiles de notificación** > **Añadir el perfil de notificación**. Esto abre el asistente **Añadir Notificación perfil**.
2. Especificar el nombre y la descripción. Haga clic en **Siguiente**.

3. Especificar destinatario, asunto, texto del mensaje y el tiempo entre mensajes de correo electrónico:



4. Para enviar una notificación de correo electrónico de prueba a los destinatarios especificados, haga clic **correo electrónico de prueba**.

5. Para incluir prealarma imágenes fijas, seleccione **Incluir imágenes**, e indique el número de imágenes, el tiempo entre las imágenes y si desea incrustar imágenes en mensajes de correo electrónico o no.

6. Para incluir clips de vídeo AVI, seleccione **Incluir AVI** y especifique el tiempo antes y después de la tasa de eventos y el marco.

Las notificaciones que contengan vídeo codificado con H.265 requieren un equipo que admita la aceleración de hardware.

7. Haga clic en **Finalizar**.

Utilizar reglas para desencadenar notificaciones por correo electrónico

Utilice la regla **Administrar** para crear reglas. El asistente le lleva a través de todos los pasos relevantes. Se especifica el uso de un perfil de notificación durante la etapa en la que se especifica acciones de la regla.

Al seleccionar acción **Enviar notificación a <perfil>**, puede seleccionar el perfil de notificación pertinente y las cámaras que cualquier grabación para incluir en las notificaciones de correo electrónico del perfil de notificaciones deben provenir de:

En **Gestionar Regla**, hace clic en los enlaces para hacer sus selecciones.

Recuerde que no se puede incluir grabaciones en las notificaciones de correo electrónico del perfil de notificaciones a menos que algo realmente está siendo grabada. Si desea que las imágenes o clips de vídeo AVI en las notificaciones de correo electrónico todavía, verificar que la regla especifica que la comprobación se efectúe. El siguiente ejemplo es de una regla que incluye tanto una acción **Iniciar grabación** y una acción **Enviar notificación a**:

Perfil de notificación (propiedades)

Especificar las siguientes propiedades de los perfiles de notificación:

Componente	Requisitos
Nombre	Escriba un nombre descriptivo para el perfil de notificación. El nombre aparece más adelante cada vez que seleccione el perfil de notificación durante el proceso de creación de una regla.
Descripción (opcional)	Escriba una descripción del perfil de notificación. La descripción aparece cuando se pasa el puntero del ratón sobre el perfil de notificación en la lista **Perfiles de notificación** de panel general.
Destinatarios	Escriba las direcciones de correo electrónico a las que se deben enviar notificaciones de correo electrónico del perfil de notificaciones. Para escribir más de una dirección de correo electrónico, direcciones separadas por punto y coma. Ejemplo: aa@aaaa.aa;bb@bbbb.bb;cc@cccc.cc
Asunto	Escriba el texto que desea que aparezca como el objeto de la notificación por correo electrónico. Puede insertar variables del sistema, como **Nombre de dispositivo**, en el campo de texto del asunto y del mensaje. Para insertar variables, haga clic en los enlaces variables necesarios en el cuadro de debajo del campo.
Mensaje de texto	Escriba el texto que desea que aparezca en el cuerpo de las notificaciones por correo electrónico. Además del texto del mensaje, el cuerpo de cada notificación de correo electrónico contiene automáticamente esta información: • Lo que provocó la notificación por correo electrónico. • La fuente de cualquier adjuntas imágenes fijas o clips de vídeo AVI

Componente	Requisitos
Tiempo entre correos electrónicos	Especificar el tiempo mínimo requerido (en segundos) que debe transcurrir entre el envío de cada una notificación por correo electrónico. Ejemplos: • Si se especifica un valor de **120**, pasar un mínimo de 2 minutos entre el envío de cada una notificación por correo electrónico, incluso si el perfil de notificación se activa de nuevo por una regla antes de que hayan transcurrido los 2 minutos. • Si se especifica un valor de **0**, se envía notificaciones por correo electrónico cada vez que el perfil de notificación es activado por una regla. Potencialmente, esto puede resultar en un número muy grande de notificaciones de correo electrónico que se envía. Si se utiliza el valor **0**, usted debe considerar cuidadosamente si, por tanto, que desea utilizar el perfil de notificación en una legislación que puede ser provocada con frecuencia.
Número de imágenes	Especificar el número máximo de imágenes fijas que desea incluir en cada una de las notificaciones de correo electrónico del perfil de notificaciones. El valor predeterminado es cinco imágenes.
Tiempo entre imágenes (ms)	Especificar el número de milisegundos que desea entre las grabaciones que se presentan en las imágenes incluidas. Ejemplo: Con el valor predeterminado de 500 milisegundos, las imágenes incluidas muestran grabaciones con medio segundo entre ellos.
Tiempo antes del evento (seg.)	Este ajuste se utiliza para especificar el inicio del archivo AVI. De manera predeterminada, el archivo AVI contiene grabaciones de 2 segundos antes de que se active el perfil de notificación. Usted puede cambiar esto a la cantidad de segundos que se requieren.
Tiempo después del evento (seg.)	Este ajuste se utiliza para especificar el final del archivo AVI. De manera predeterminada, el archivo AVI acaba en 4 segundos después de que el perfil de notificación se activa. Usted puede cambiar esto a la cantidad de segundos que se requieren.
Velocidad de fotogramas	Especificar el número de fotogramas por segundo que desea el archivo AVI a contener. El valor predeterminado es cinco fotogramas por segundo. Cuanto mayor sea la frecuencia de imagen, mayor será la calidad de imagen y tamaño del archivo AVI.
Incrustar imágenes en correo electrónico	Si es seleccionado (por defecto), las imágenes se insertan en el cuerpo de notificaciones por correo electrónico. Si no, las imágenes se incluyen en las notificaciones de correo electrónico como archivos adjuntos.

Eventos definidos por el usuario

Eventos definidos por el usuario (explicados)

Si el evento que necesita no está en la lista **Eventos generales**, puede crear sus propios eventos definidos por el usuario. Utilice este tipo de eventos definidos por el usuario para integrar otros sistemas con su sistema de vigilancia.

Con eventos definidos por el usuario, puede utilizar los datos recibidos desde un sistema de control de acceso de terceros como los acontecimientos en el sistema. Los acontecimientos posteriores pueden desencadenar acciones. De esta manera, se puede, por ejemplo, iniciar la grabación de vídeo de las cámaras pertinentes cuando alguien entra en un edificio.

También puede utilizar los eventos definidos por el usuario para los eventos de activación de forma manual mientras se visualiza vídeo en directo en el XProtect Smart Client o automáticamente si se utilizan en las reglas. Por ejemplo, cuando se produce un evento definido por el usuario 37, la cámara PTZ 224 debe dejar de patrullaje e ir a la posición preestablecida 18.

A través de los cometidos, se define qué usuarios son capaces de desencadenar los eventos definidos por el usuario. Puede usar los eventos definidos por el usuario de dos maneras y, al mismo tiempo, si es necesario:

Eventos	Descripción
Para proporcionar la capacidad de activar manualmente eventos en XProtect Smart Client	En este caso, los eventos definidos por el usuario hacen posible que los usuarios finales para activar manualmente los eventos durante la visualización de vídeo en directo en el XProtect Smart Client. Cuando se produce un evento definido por el usuario porque un usuario de XProtect Smart Client acciona de forma manual, una regla puede provocar que una o más acciones deben llevarse a cabo en el sistema.

Eventos	Descripción
Para proporcionar la capacidad de desencadenar eventos a través de la API	En este caso, puede desencadenar eventos definidos por el usuario fuera del sistema de vigilancia. El uso de eventos definidos por el usuario de esta manera requiere que un API independiente (Application Program Interface. Un conjunto de bloques de construcción para la creación o la personalización de las aplicaciones de software) se utiliza cuando se activa el evento definido por el usuario. Se requiere la autenticación a través de Active Directory para el uso de eventos definidos por el usuario de esta manera. Esto asegura que incluso si los eventos definidos por el usuario se pueden activar desde fuera del sistema de vigilancia, sólo los usuarios autorizados para hacerlo. Además, los eventos definidos por el usuario pueden estar asociados a través de la API con meta-datos, definir ciertos dispositivos o grupos de dispositivos. Esto es muy fácil de utilizar cuando se utilizan los eventos definidos por el usuario para activar reglas: a evitar tener una regla para cada dispositivo, haciendo básicamente lo mismo. Ejemplo: Una empresa utiliza el control de acceso, que tiene 35 entradas, cada una con un dispositivo de control de acceso. Cuando se activa un dispositivo de control de acceso, un evento definido por el usuario se activa en el sistema. Este evento definido por el usuario se utiliza en una regla para iniciar la grabación en una cámara asociada con el dispositivo de control de acceso activado. Se define en el meta-datos de la cámara que está asociada con qué regla. De esta manera la empresa no necesita tener 35 eventos definidos por el usuario y las 35 reglas desencadenadas por los eventos definidos por el usuario. Un evento definido por el usuario único y una sola regla son suficientes. Cuando se utiliza eventos definidos por el usuario de esta manera, puede que no siempre desea que estén disponibles para el disparo manual de XProtect Smart Client. Puede utilizar cometidos para definir qué eventos definidos por el usuario deben ser visibles en XProtect Smart Client.

No importa la forma en que desea utilizar eventos definidos por el usuario, debe añadir cada evento definido por el usuario a través del Management Client.

Si cambia el nombre de un evento definido por el usuario, los usuarios de XProtect Smart Client ya conectado deben desconectarse y conectarse de nuevo antes de que el cambio de nombre es visible.

También tenga en cuenta que si se elimina un evento definido por el usuario, esto afecta a cualquier regla en la que el evento definido por el usuario está en uso. Además, un evento definido por el usuario eliminado solamente desaparece de XProtect Smart Client cuando los usuarios XProtect Smart Client se desconectan.

Añadir un evento definido por el usuario

1. Expandir **Reglas y Eventos** > **Eventos definidos por el usuario**.
2. En el panel **general**, haga clic **Eventos** > **Añadir evento definido por el usuario**.
3. Escriba un nombre para el nuevo evento definido por el usuario, y haga clic en **OK**. El evento definido por el usuario recién agregado aparece ahora en la lista en el panel **general**.
4. Ahora el usuario puede activar el evento definido por el usuario de forma manual en el XProtect Smart Client si el usuario tiene derechos para hacerlo.

Cambiar el nombre de un evento definido por el usuario

1. Expandir **Reglas y Eventos** > **Eventos definidos por el usuario**.
2. En el panel **general**, seleccione el evento definido por el usuario.
3. En el panel **Propiedades**, sobrescribir el nombre existente.
4. En la barra de herramientas, haga clic en **Guardar**.

Eventos analíticos

Eventos de Google Analytics (explicados)

Los eventos de Analytics son normalmente datos recibidos de proveedores externos de análisis de contenido de video (VCA) de terceros.

El uso de eventos analíticos como base para las alarmas es básicamente un proceso de tres pasos:

- La primera parte, lo que permite el cuentan Eventos de Analytics y la creación de su seguridad. Utilice una lista de direcciones permitidas para controlar quién puede enviar datos de eventos al sistema y qué puerto escucha el servidor.
- La segunda parte, crear el evento de analytics, posiblemente con una descripción del evento, y prueba de ello.
- La tercera parte, utilizando el evento de analytics como la fuente de una definición de alarma.

Se configura eventos de analytics sobre las **Reglas y Eventos** lista en el panel de **navegación del sitio**.

Para utilizar los eventos basados en VCA, se requiere una herramienta VCA de terceros para el suministro de datos al sistema. ¿Qué herramienta VCA a utilizar es totalmente de usted, siempre y cuando los datos suministrados por la herramienta se adhieren al formato. Este formato se establece en Milestone Analytics Events: Manual del Desarrollador. Póngase en contacto con su proveedor de sistema para obtener más detalles, Herramientas VCA terceros son desarrollados por socios independientes que entregan soluciones basadas en una plataforma abierta de Milestone. Estas soluciones pueden afectar al rendimiento del sistema.

Añadir y editar un evento analítico

Añadir un evento analítico

1. Expandir **Reglas y Eventos**, haga clic **Eventos analíticos** y seleccione **Añadir nuevo**.
2. Enventana, **Propiedades** escriba un nombre para el evento en el campo **Nombre**.
3. Escriba un texto de descripción en el campo **Descripción** si es necesario.
4. En la barra de herramientas, haga clic en **Guardar**. Puede probar la validez del evento haciendo clic **Evento de prueba**. Puede errores continuamente correctos indicadas en la prueba y ejecutar la prueba tantas veces como desee y desde cualquier parte del proceso.

Editar un evento analítico

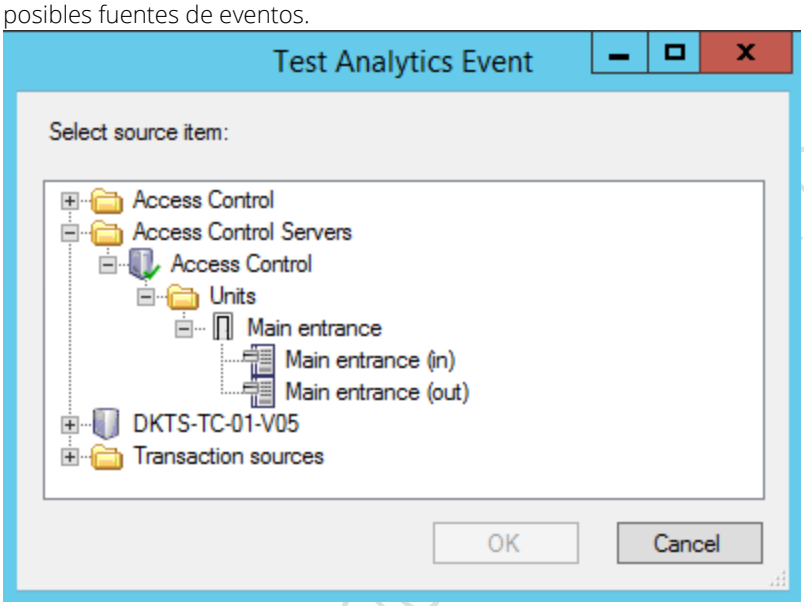
1. Haga clic en un evento de analytics existentes para acceder a las **propiedades** ventana, donde puede editar los campos pertinentes.

2. Puede probar la validez del evento haciendo clic en **Evento de prueba**. Puede errores continuamente correctos indicadas en la prueba y ejecutar la prueba tantas veces como desee y desde cualquier parte del proceso.

Pruebe un evento de análisis

Después de crear un evento de análisis, puede probar los requisitos (ver "Prueba de Análisis de Eventos (propiedades)" en la página 221), por ejemplo, que la característica de evento analítico se ha habilitado en Management Client.

1. Selecciona un evento de analytics existentes.
2. En las propiedades, haga clic en el botón **Probar evento**. Aparece una ventana que muestra todas las posibles fuentes de eventos.



3. Seleccione la fuente de su evento de prueba, por ejemplo una cámara. La ventana se cierra y aparece una nueva ventana que pasa por cuatro condiciones que deben cumplirse para el evento de analytics funcione.

Como prueba adicional, en XProtect Smart Client puede comprobar que el evento analítico fue enviado al servidor de eventos. Para ello, abra XProtect Smart Client y ver el evento en la ficha **Administrador de alarmas**.

Ver también

Eventos de Google Analytics (explicados) (en la página 220)

Prueba de Análisis de Eventos (propiedades)

Al probar los requisitos de un evento de analytics, aparece una ventana que comprueba cuatro condiciones posibles y proporciona descripciones y soluciones de errores.

Condición	Descripción	Los mensajes de error y soluciones
Cambios guardados	Si el evento es nuevo, se salvó? O si hay cambios en el nombre del evento, se guardan estos cambios?	**Guardar cambios antes de probar el evento de análisis** Solución/Explicación: Guardar cambios.

Condición	Descripción	Los mensajes de error y soluciones
Eventos analíticos activados	Se habilita la función de Evento de Analytics?	**No se han habilitado los eventos de Analytics.** Solución / Explicación: Habilitar el función Eventos de Analytics. Para ello, haga clic en **Herramientas** > **Opciones** > **Eventos de analytics** y seleccione la casilla de verificación **Habilitado**.
Dirección permitida	Es la dirección IP / nombre de host del envío del evento (s) permitido (que aparece en la lista de direcciones de eventos analíticos) máquina?	**El nombre de host local debe añadirse como dirección permitida para el servicio Analytics Event.**Solución / Explicación: Añadir el dispositivo a la lista de direcciones de eventos analitico de direcciones permitidos IP o nombres de host. **Error al resolver el nombre de host local.** Solución / Explicación: La dirección IP o nombre de host de la máquina no se encuentran o no son válidos.
Enviar un evento analítico	¿Se envía un evento de prueba al servidor de eventos tienen éxito?	Vea la tabla a continuación.

Cada etapa está marcada por cualquiera fallido: ✗ o exitoso: ✓.

Los mensajes de error y soluciones para el evento condición **Enviar evento de analytics**:

Servidor de eventos no encontrado	No se puede encontrar el servidor de eventos en la lista de servicios registrados.
Error al conectar con el servidor de eventos	No se puede conectar al servidor de eventos en el puerto indicado. Se produce el error más probable debido a problemas en la red, o el servicio de servidor de eventos se ha detenido.
Error al enviar el evento analítico	La conexión con el servidor de eventos se establece, pero el evento no puede ser enviado. El error más probable se produce debido a problemas de red, por ejemplo, un tiempo de espera.
Error al recibir respuesta del servidor de eventos	El evento ha sido enviado al servidor de eventos, pero no recibió respuesta alguna. El error más probable se produce debido a problemas de red o un puerto que está ocupado. Ver el registro del servidor de eventos, normalmente situada en ProgramData\Milestone\XProtect Event Server\logs\.
Evento analítico desconocido por el servidor de eventos	El servicio de servidor de eventos no conoce el caso. El error más probable se debe a que el evento o cambios a la cita no se han guardado.
Evento analítico no válido recibido por el servidor de eventos	El formato del evento es incorrecto.
Remitente no autorizado por parte del servidor de eventos	Lo más probable es que su máquina no está en la lista de direcciones IP o nombres de host permitidos.

Error interno en el servidor de eventos.	Error del servidor de eventos. Ver el registro del servidor de eventos, normalmente situada en ProgramData\Milestone\XProtect Event Server\logs\.
Respuesta no válida recibida del servidor de eventos	La respuesta no es válida. Posiblemente el puerto está ocupado o si hay problemas en la red. Ver el registro del servidor de eventos, normalmente situada en ProgramData\Milestone\XProtect Event Server\logs\.
Respuesta desconocida del servidor de eventos	La respuesta es válida, pero no se entiende. El error se produce posiblemente debido a problemas en la red, o el puerto está ocupado. Ver el registro del servidor de eventos, normalmente situada en ProgramData\Milestone\XProtect Event Server\logs\.
Error inesperado	Por favor, póngase en contacto con Milestone asistencia para obtener ayuda.

Editar la configuración de eventos analíticos

En la barra de herramientas, vaya a las **Herramientas** > **Opciones** > pestaña **Eventos analíticos** para editar los ajustes pertinentes.

Eventos genéricos

Eventos genéricos (explicados)

Importante: Esta característica no funciona si no tiene instalado el servidor de eventos XProtect.

Eventos genéricos le permiten activar acciones en el servidor de eventos XProtect mediante el envío de cadenas simples a través de la red IP para su sistema.

Se puede utilizar cualquier hardware o software, que puede enviar cadenas a través de TCP o UDP, para activar eventos genéricos. Su sistema puede analizar TCP recibido o paquetes de datos UDP, y automáticamente activar eventos genéricos cuando se cumplan criterios específicos. De esta manera, es posible integrar el sistema con fuentes externas, por ejemplo, los sistemas de control de acceso y sistemas de alarma. El objetivo es permitir que el mayor número de fuentes externas como sea posible para interactuar con el sistema.

Con el concepto de fuentes de datos, se evita tener que adaptar las herramientas de terceros para cumplir con las normas de su sistema. Con fuentes de datos, puede comunicarse con una determinada pieza de hardware o software en un puerto específico IP y afinar cómo se interpretan los bytes que llegan en ese puerto. Cada genéricos pares tipo de evento con una fuente de datos y conforma un idioma que se utiliza para la comunicación con una pieza específica de hardware o software.

Trabajar con fuentes de datos requiere un conocimiento general de las redes IP y el conocimiento específico del software individual dura o desea interconectar a partir. Hay muchos parámetros que puede utilizar y sin solución lista para usar sobre cómo hacer esto. Básicamente, el sistema proporciona las herramientas, pero no la solución. A diferencia de los eventos definidos por el usuario, eventos genéricos tienen ninguna autenticación. Esto hace que sean más fáciles de gatillo, pero, para evitar poner en peligro la seguridad, sólo se aceptan los eventos de host local. Puede permitir que otras direcciones IP de los clientes de la **Eventos Genéricas** pestaña del menú **Opciones**.

Añadir un evento genérico

Puede definir eventos genéricos para ayudar al VMS a reconocer cadenas específicas en paquetes TCP o UDP desde un sistema externo. Sobre la base de un evento genérico, puede configurar Management Client para desencadenar acciones, por ejemplo, para iniciar la grabación, o alarmas.

Requisitos
Ha habilitado eventos genéricos y especifica los destinos permitidos de origen. Para más información, ver Pestaña Eventos genéricos (ver "Pestaña eventos genéricas (opciones)" en la página 291).

Para agregar un evento genérico:

1. Expandir **Reglas y Eventos**.
2. Haga clic con **Eventos Genéricas** y seleccione **Añadir nuevo**.
3. Llene la información y las propiedades necesarias. Para obtener más información, consulte Propiedades de eventos genéricos (ver "Evento genérico (propiedades)" en la página 224).
4. (Opcional) Para validar que la expresión de búsqueda es válida, introduzca una cadena de búsqueda en el **Comprobar si la expresión coincide con la cadena de eventos** campo que corresponde a los paquetes esperados:
   - **Coincidencia** - la cadena puede ser validado en contra de la expresión de búsqueda.
   - **Sin coincidencia** - la expresión de búsqueda no es válida. Cambiarlo y volver a intentarlo.

En XProtect Smart Client, se puede verificar si sus eventos genéricos han sido recibidos por el servidor de eventos. Esto se hace en la **Lista alarma** en la ficha **Administrador de alarmas** seleccionando **Eventos**.

Evento genérico (propiedades)

Componente	Requisitos
Nombre	Nombre único para el evento genérico. El nombre debe ser único entre todos los tipos de eventos, tales como eventos definidos por el usuario, eventos analíticos, y así sucesivamente.
Habilitado	Eventos genéricos están habilitadas de forma predeterminada. Desactive la casilla de verificación para desactivar el evento.

Expresión	Expresión que el sistema debe tener en cuenta al analizar los paquetes de datos. Se pueden utilizar los siguientes operadores: • **( ):** Se utiliza para garantizar que los términos relacionados se procesan juntos como una unidad lógica. Pueden ser utilizados para forzar un cierto orden de procesamiento en el análisis. **Ejemplo:** Los criterios de búsqueda "(**User001** OR **Door053**) AND **Domingo**" primero procesa los dos términos dentro del paréntesis y, a continuación, combina el resultado con la última parte de la cadena. Por lo tanto, el sistema busca primero los paquetes que contengan cualquiera de los términos **User001** o **Door053**, luego toma los resultados y correr a través de ellos con el fin de ver que también paquetes contienen el término **Domingo**. • **Y:** Con un operador AND, se especifica que los términos en ambos lados del operador AND deben estar presentes. **Ejemplo:** Los criterios de búsqueda "**User001** Y **Door053** Y **Domingo**" devuelve un resultado sólo si los términos **User001**, **Door053** y **Domingo** están todos incluidos en su expresión. No es suficiente para sólo uno o dos de los términos que se presente. Cuantos más términos se combinan con el Y, el menor número de resultados que se recuperen. • **OR:** Con un operador tiene la opción de especificar que sea uno u otro término debe estar presente. **Ejemplo:** Los criterios de búsqueda "**User001** OR **Door053** OR **Domingo**" devuelve cualquier resultado que contenga **User001**, **Door053** o **Domingo**. Cuantos más términos se combinan con O, más resultados que recuperar.
Tipo de expresión	Indica la forma en particular, el sistema debe ser la hora de analizar los paquetes de datos recibidos. Las opciones son las siguientes: • **Búsqueda:** Con el fin de que ocurra el evento, el paquete de datos recibido debe contener el texto especificado en el campo **Expresión:**, pero también puede tener más contenido. **Ejemplo:** Si ha especificado que el paquete recibido debe contener los términos **User001** y **Door053**, el evento se activa si el paquete recibido contiene los términos **User001** y **Door053** y **Domingo** ya que sus dos términos requeridos están contenidos en el paquete recibido. • **Partido:** A fin de que el evento ocurra, el paquete de datos recibido debe contener exactamente el texto especificado en la campo **Expresión:**, y nada más. • **Expresión regular:** A fin de que el evento ocurra, el texto especificado en el campo **Expresión**: debe identificar patrones específicos en los paquetes de datos recibidos. Si cambia de **Búsqueda** o **Coincidencia** para **Expresión regular**, el texto en el campo **Expresión** se traduce automáticamente en una expresión regular.

Prioridad	La prioridad debe especificarse como un número entre 0 (prioridad más baja) y 999999 (prioridad más alta). El mismo paquete de datos puede ser analizado para diferentes eventos. La posibilidad de asignar una prioridad a cada evento le permite administrar cuyo caso debe activarse si un paquete recibido coincide con los criterios de varios eventos. Cuando el sistema recibe un TCP y / o el paquete UDP, el análisis del paquete comienza con el análisis para el evento con la prioridad más alta. De esta manera, cuando un paquete coincide con los criterios de varios eventos, sólo el evento de mayor prioridad se activa. Si un paquete coincide con los criterios de varios eventos con una prioridad idéntica, por ejemplo, dos eventos con una prioridad de 999, todos los eventos con esta prioridad se activan.
Compruebe si la expresión coincide con la cadena de eventos	Una cadena de eventos para confrontarse con la expresión introducida en el campo **Expresión:**.

Fuente de datos de eventos genérico (propiedades)

Componente	Requisitos
Fuente de datos	Se puede elegir entre dos fuentes de datos por defecto y definir una fuente de datos personalizada. ¿Qué a elegir depende de su programa de terceros y / o el hardware o software que desea interactuar a partir de: **Compatible:** Valores predeterminados de fábrica están activados, se hace eco de todos los bytes, TCP y UDP, sólo Ipv4, el puerto 1234, ningún separador, anfitrión local solamente, la página de códigos actual codificación (ANSI). **Internacional:** Valores predeterminados de fábrica están activados, se hace eco de estadísticas sólo, sólo TCP, Ipv4+6, el puerto 1235, <CR> <LF> como separador, anfitrión local solamente, codificación UTF-8. (<CR> <LF> = 13,10). [Fuente de C Datos] [Fuente de datos B] y así.
Nuevo	Haga clic para crear una nueva fuente de datos.
Nombre	Nombre del origen de datos.
Habilitado	Las fuentes de datos están habilitadas de forma predeterminada. Desactive la casilla de verificación para desactivar la fuente de datos.
restablecer	Haga clic para restablecer todos los ajustes para la fuente de datos seleccionada. El nombre introducido en el campo **Nombre** permanece.
Puerto	El número de puerto de la fuente de datos.

Componente	Requisitos
Selector de tipo de protocolo	Protocolos que el sistema debe escuchar a, y analizar, con el fin de detectar eventos genéricos: **Cualquier:** TCP, así como UDP. **TCP:** TCP solamente. **UDP:** UDP solamente. Paquetes TCP y UDP utilizados para eventos genéricos pueden contener caracteres especiales, como @, #, +, ~, y más.
selector de tipo IP	Seleccionables tipos de direcciones IP: IPv4, IPv6 o ambos.
Bytes separadoras	Seleccione los bytes de separación utilizados Para separar los registros de eventos genéricos individuales. Predeterminado para el tipo de fuente de datos **Internacional** (ver **Fuentes de datos** anterior) es **13,10**. (13,10 = <CR><IF>).
Selector del tipo de eco	Disponibles formatos de retorno del eco: • **Estadísticas de eco:** Se hace eco el siguiente formato: **[X], [Y], [Z], [Nombre del evento genérico]** **[X]** = número de solicitud. **[Y]** = número de caracteres. **[Z]** = número de partidos con un evento genérico. **[Nombre del evento genérico]** = nombre inscrito en el campo **Nombre**. • **Echo todos los bytes:** Se hace eco de todos los bytes. • **Sin eco:** Suprime todos los ecos.
Selector de tipo de codificación	Por defecto, la lista sólo muestra las opciones más relevantes. Seleccione la casilla verificación **Mostrar todo** para mostrar todas las codificaciones disponibles.
Mostrar todo	Consulte el apartado anterior.
Las direcciones IPv4 externos permitidos	Especificar las direcciones IP, que el servidor de gestión debe ser capaz de comunicarse con el fin de gestionar los eventos externos. También puede usar esto para excluir direcciones IP que no desea datos.
Se admiten direcciones IPv6 externos	Especificar las direcciones IP, que el servidor de gestión debe ser capaz de comunicarse con el fin de gestionar los eventos externos. También puede usar esto para excluir direcciones IP que no desea datos.

Consejo: Los rangos pueden ser especificados en cada una de las cuatro posiciones, como **100,105,110-120**. A modo de ejemplo, todas las direcciones de la red 10,10 se puede permitir por **10,10.[0-254].[0-254]** o por **10.10.255.255**.

Seguridad

Cometidos

Cometidos (explicados)

Los cometidos determinan qué dispositivos pueden acceder los usuarios. Cometidos también determinan los derechos y manejar la seguridad dentro del sistema de gestión de vídeo. En primer lugar, se agrega cometidos, a continuación, añadir usuarios y grupos y, finalmente, un Smart Client y un perfil de Management Client, así como otros perfiles predeterminados que pertenecen a cada cometido. Los cometidos que se pueden crear en el sistema tienen sus propios grupos de vistas de XProtect Smart Client en el que se crean y almacenan sus vistas.

El sistema viene con un rol predefinido que no se puede eliminar: el cometido **Administradores**. Los usuarios y grupos con el cometido **Administradores** tienen acceso completo y sin restricciones a todo el sistema. Por este motivo, no puede especificar la Configuración de cometido para el cometido **Administradores**. El cometido **Administradores** tiene el perfil de Smart Client defecto y los perfiles de bloqueo de evidencia por defecto y no tiene un perfil temporal.

Los usuarios con derechos de administrador de equipo local en el equipo que ejecuta el servidor de gestión automática tienen derechos de administrador en el servidor de gestión. Sólo los usuarios que confía como administradores de su sistema debe tener derechos de administrador de equipo local en el equipo que ejecuta el servidor de gestión. No se puede desactivar esta opción. Añadir usuarios y grupos al cometido **Administradores** al igual que con cualquier otro cometido. Ver Asignar y eliminar usuarios y grupos de / a los cometidos (ver "Asignar / eliminar usuarios y grupos a / desde los cometidos" en la página 231).

Además de la función **Administradores**, puede añadir tantos cometidos como sea necesario para satisfacer sus necesidades. Es posible, por ejemplo, tienen diferentes cometidos para los usuarios de XProtect Smart Client dependiendo de qué cámaras que desea que tengan acceso o restricciones similares. Para configurar cometidos en su sistema, expanda el **Seguridad** > **Cometidos**.

Derechos de un cometido (explicado)

Funcionalidad disponible depende del sistema que está utilizando. Ver tabla de comparación de productos (en la página 24) para más información.

Cuando se crea un cometido en su sistema, puede dar al cometido una serie de derechos a los componentes del sistema o características que el cometido relevante que puede acceder y utilizar. Por ejemplo, puede crear cometidos que sólo tengan derechos de funcionalidad en XProtect Smart Client u otros Milestone que vean clientes, con derechos para ver sólo ciertas cámaras. Si crea esas cometidos, estas cometidos no deben tener derechos de acceso y uso del Management Client, pero sólo tienen acceso a una parte o toda la funcionalidad que se encuentra en XProtect Smart Client u otros clientes. Para hacer frente a esto, es posible que desee configurar un cometido que tiene unas o más típicos derechos de administrador, por ejemplo, los derechos para añadir y eliminar cámaras, servidores y una funcionalidad similar.

Puede crear cometidos que tienen algunos o la mayoría de los derechos de un administrador del sistema. Esto puede, por ejemplo, ser relevante si su organización quiere separar entre las personas que pueden administrar un subconjunto del sistema y las personas que pueden administrar todo el sistema. La característica le permite proporcionar permisos de administrador diferenciadas para acceder, modificar o cambiar una gran variedad de funciones del sistema, por ejemplo, el derecho a editar la configuración de los servidores y cámaras en su sistema. Especifique estos permisos en la pestaña Seguridad general (ver "Pestaña de Seguridad General (cometidos)" en la página 234). Como mínimo, para permitir que el administrador del sistema puede lanzar

diferenciado del Management Client, debe conceder permisos de lectura en el servidor de gestión para el cometido.

También puede reflejar las mismas limitaciones en la interfaz de usuario del Management Client para cada cometido mediante la asociación del cometido con un perfil de Management Client que se ha eliminado el que funciona el sistema correspondiente de la interfaz de usuario. Consulte perfiles Management Client (explicados) (en la página 179) para obtener información.

Para otorgarle un cometido de derechos de administrador diferenciados, la persona con el rol de administrador completo predeterminado debe configurar el cometido en **Seguridad** > **Cometidos > ficha Información > Añadir nuevo**. Al configurar el nuevo cometido, a continuación, puede asociar el cometido con sus propios perfiles deben de manera similar a cuando se configura cualquier otro cometido en el sistema o utilizar los perfiles predeterminados del sistema. Para obtener más información, consulte Adición y gestión de un cometido (ver "Añadir y gestionar un cometido" en la página 230).

Una vez que haya especificado qué perfiles que desea asociar con el cometido, vaya a la pestaña de **seguridad general** para especificar los derechos de la función.

Los derechos se pueden establecer para un cometido son diferentes entre sus productos. Sólo se puede dar todos los derechos disponibles para un cometido en XProtect Corporate.

Usuarios (explicado)

El término **usuarios** se refiere principalmente a los usuarios que se conectan al sistema de vigilancia a través de los clientes. Puede configurar este tipo de usuarios de dos maneras:

- Como **usuarios básicos**, autenticadas por una combinación de nombre de usuario / contraseña.
- A medida que los **usuarios de Windows** autenticados, en función de su inicio de sesión de Windows.

Usuarios de windows

Agrega usuarios de Windows mediante el uso de Active Directory. Active Directory (AD) es un servicio de directorio Implementado por Microsoft para Dominio de Windows redes. Está incluido en la mayoría de Windows Server sistemas operativos. Identifica los recursos en una red para que los usuarios o aplicaciones para acceder a ellos. Active Directory utiliza los conceptos de usuarios y grupos.

Los usuarios son objetos de Active Directory que representan a las personas con una cuenta de usuario. Ejemplo:

Los grupos son objetos de Active Directory con varios usuarios. En este ejemplo, el Grupo de Gestión tiene tres usuarios:

Los grupos pueden contener cualquier número de usuarios. Mediante la adición de un grupo al sistema, se agrega a todos sus miembros de una sola vez. Una vez que haya agregado el grupo al sistema, cualquier cambio realizado en el grupo en Active Directory, como los nuevos miembros que se agregan o antiguos miembros de quitar en una etapa posterior, se reflejan inmediatamente en el sistema. Tenga en cuenta que un usuario puede ser miembro de más de un grupo a la vez.

Puede utilizar Active Directory para añadir información de usuarios y grupos existentes en el sistema con algunas ventajas:

- Los usuarios y grupos se especifica en el centro de Active Directory por lo que no tiene que crear cuentas de usuario desde cero.
- Usted no tiene que configurar ningún tipo de autenticación de usuarios en el sistema como Active Directory controla la autenticación.

Antes de añadir usuarios y grupos a través del servicio de Active Directory, debe tener un servidor con Active Directory instalado en su red.

Usuarios básicos

Si su sistema no tiene acceso a Active Directory, cree un usuario básico (ver "Usuarios básicos (explicado)" en la página 261). Para obtener información acerca de cómo configurar los usuarios básicos, consulte Crear usuario básico (ver "Crear usuarios básicos" en la página 261).

Añadir y gestionar un cometido

1. Expandir **Seguridad** y haga clic derecho **Cometidos**.
2. Seleccione **Añadir cometido**. Esto abre el cuadro de diálogo **Añadir cometido**.
3. Escriba un nombre y una descripción de la nueva función y haga clic en **OK**.
4. El nuevo rol se agrega a la lista **Cometidos**. Por defecto, un nuevo cometido no tiene ningún usuarios / grupos asociados a ella, pero tiene una serie de perfiles predeterminados asociados.
5. Para elegir diferentes perfiles de Smart Client y Management Client perfiles de bloqueo de evidencia o perfiles temporales, haga clic en las listas desplegables.
6. Ahora puede asignar usuarios / grupos para el cometido, y especificar cuál de las características del sistema que pueden acceder.

Ver también Asignar / eliminar usuarios y grupos a / desde los cometidos (en la página 231) y Configuración de cometido (ver "Configuración cometidos" en la página 232).

Copiar, renombrar o borrar un cometido

Copiar un cometido

Si usted tiene un cometido con configuraciones complicadas y / o derechos y la necesidad de un cometido similar o casi similar, podría ser más fácil copiar el cometido ya existente y hacer ajustes menores a la copia que a la creación de un nuevo cometido a partir de cero.

1. Expandir **Seguridad**, haga clic en **Cometidos**, haga clic con el cometido relevante y seleccione **Copiar cometido**.
2. En el cuadro de diálogo que se abre, darle el cometido copiado un nuevo nombre y una descripción únicos.

3. **Haga clic en OK (aceptar)**.

Cambiar el nombre de un cometido

Si cambia el nombre de una función, esto no cambia el nombre del grupo de vista basado en el del cometido.

1. Expandir **Seguridad** y, haga clic en **cometidos**.
2. Haga clic con el cometido que desee y seleccione **Renombrar cometido**.
3. En el cuadro de diálogo que se abre, cambie el nombre de la función.
4. **Haga clic en OK (aceptar)**.

Eliminar un cometido

1. Expandir **Seguridad**, y haga clic en **Cometidos**.
2. Haga clic con el cometido deseado y seleccione **Eliminar cometido**.
3. Haga clic en **Sí**.

Importante: Si elimina una función, esto no elimina el grupo de vista basado en el del cometido.

Asignar / eliminar usuarios y grupos a / desde los cometidos

Para asignar o eliminar usuarios o grupos de windows o usuarios básicos a / de un cometido:

1. Expanda **Seguridad** y seleccione **Cometidos**. A continuación, seleccione el cometido requerido en el panel **general**:
2. En el panel **Propiedades**, seleccione pestaña **Usuarios y grupos** en la parte inferior.
3. Haga clic en **Añadir**, seleccione entre **usuario de Windows** o **usuario básico**.

Asignar usuarios y grupos de Windows a un cometido

1. Seleccione **usuario de Windows**. Esto abre las **Seleccionar usuarios**, cuadro de diálogo **Computadoras y Grupos**:
2. Compruebe que se especifica el tipo de objeto requerido. Si, por ejemplo, necesita añadir un equipo, haga clic en **Tipos de objetos** y marque **Equipo**. Compruebe también que el dominio requerido se especifica en el campo **Desde esta ubicación**. Si no es así, haga clic en **Ubicaciones** para buscar el dominio deseado.
3. En el cuadro **Introduzca los nombres de objeto para seleccionar**, escriba los nombres de usuario relevantes, las iniciales u otros tipos de identificador que Active Directory pueda reconocer. Utilice la característica **Comprobar nombres** para comprobar que Active Directory reconoce los nombres o las iniciales que ha escrito. Como alternativa, utilice el función **Avanzados** para buscar usuarios o grupos.
4. Haga clic en **OK**. Los usuarios / grupos seleccionados se agregan ahora a la lista de usuarios de la pestaña **Usuarios y grupos** a los que ha asignado la función seleccionada. Se pueden añadir más usuarios y grupos mediante la introducción de múltiples nombres separados por un punto y coma (**;**).

Asignar a los usuarios básicos a un cometido

1. Seleccione **Usuario básico**. Esto abre las **Seleccionar usuarios básicos para añadir a cometido** cuadro de diálogo:
2. Seleccione el usuario básico (s) que desea asignar a esta función.
3. Opcional: Haga clic en **Nueva** para crear un nuevo usuario básico.
4. Haga clic en **OK**. El usuario básico seleccionado (s) ahora se añaden a pestaña **Usuarios y grupos** lista de usuarios básicos que se ha asignado el rol seleccionado.

Eliminar usuarios y grupos a partir de un cometido

1. En la ficha **Usuarios y grupos**, seleccione el usuario o grupo que desea eliminar y haga clic en **Quite** en la parte inferior de la ficha. Puede seleccionar más de un usuario o grupo, o una combinación de grupos y usuarios individuales, si es necesario.
2. Confirme que desea eliminar el usuario seleccionado (s) o y el grupo (s). Haga clic en **Sí**.

Un usuario también puede tener un cometido a través de la pertenencia a grupos. Cuando ese es el caso, no se puede quitar el usuario individual del cometido. Los miembros del grupo también pueden tener cometidos como individuos. Para averiguar qué usuarios de cometidos, grupos, o los miembros del grupo han, utilizar las función **Ver los cometidos efectivas**.

Ver un cometido efectivo

Con la función de un cometido efectivo, se puede ver todos los cometidos de un usuario o grupo seleccionado. Esto es práctico si está utilizando grupos y es la única forma de ver qué cometidos de un usuario específico es un miembro de.

1. Abrir ventana **cometidos efectivos** mediante la ampliación de **Seguridad** , a continuación, haga clic en **Cometidos y seleccione un cometido efectivo** .
2. Si desea información sobre un usuario básico, escriba el nombre en el campo **Nombre de usuario**. Haga clic en **Actualizar** para mostrar los cometidos del usuario.
3. Si utiliza usuarios o grupos de Windows en Active Directory, haga clic en el botón de búsqueda "**" ... "**. Seleccione el tipo de objeto, introduzca el nombre y haga clic en **OK**. Los cometidos del usuario aparecen automáticamente.

Configuración cometidos

Pestaña Información (cometidos)

Funcionalidad disponible depende del sistema que está utilizando. Ver tabla de comparación de productos (en la página 24) para más información.

En la pestaña **información** de un cometido, se puede establecer lo siguiente:

Nombre	Descripción
Nombre	Escriba un nombre para el cometido.
Descripción	Escriba una descripción para el cometido.

Nombre	Descripción
Perfil Management Client	Seleccionar un perfil de Management Client para asociarse con el cometido. No se puede aplicar esto a la forma predeterminada **Administradores** cometido. Requiere permisos para administrar la seguridad en el servidor de gestión.
Perfil Smart Client	Seleccionar un perfil de Smart Client para asociarse con el cometido. Requiere permisos para administrar la seguridad en el servidor de gestión.
Perfil temporal predeterminado	Seleccionar un perfil temporal predeterminado para asociarse con el cometido. No se puede aplicar esto a la forma predeterminada **Administradores** cometido.
Perfil de bloqueo de evidencias	Seleccionar un perfil de bloqueo de pruebas para asociarse con el cometido.
Smart Client inicio de sesión dentro del perfil temporal	Seleccionar un perfil temporal durante el cual se permite al usuario XProtect Smart Client asociado a esta función para iniciar sesión. Si el usuario XProtect Smart Client cuando se registra en el plazo expira, él o ella se cierra automáticamente. No se puede aplicar esto a la forma predeterminada **Administradores** cometido.
Permitir inicio de sesión Smart Client	Seleccione la casilla de verificación para permitir que los usuarios asociados a esta función inicien sesión en XProtect Smart Client. El acceso a Smart Client está permitido por defecto. Desactive la casilla de verificación para denegar el acceso a XProtect Smart Client.
Permitir Milestone Mobile inicio de sesión de cliente	Seleccione la casilla de verificación para permitir que los usuarios asociados a esta función inicien sesión en Milestone Mobile Client. El acceso a Milestone Mobile Cliente está permitido por defecto. Desactive la casilla de verificación para denegar el acceso a cliente Milestone Mobile.
Permitir XProtect Web Client inicio de sesión	Active la casilla de verificación para permitir que los usuarios asociados a esta función inicien sesión en XProtect Web Client. El acceso a XProtect Web Client está permitido por defecto. Desactive la casilla de verificación para denegar el acceso a XProtect Web Client.
Es necesaria la autorización del inicio de sesión	Seleccione la casilla de verificación para asociar la autorización de acceso a la función. Esto significa que XProtect Smart Client o el Management Client pide una segunda autorización, normalmente por un superusuario o administrador, cuando el usuario inicie sesión. Para permitir a los administradores autorizar a los usuarios, configurar **Usuarios Autorizados** del servidor de gestión derecho en la pestaña de **Seguridad general**. No se puede aplicar esto a la forma predeterminada **Administradores** cometido.

Nombre	Descripción
Hacer que los usuarios sean anónimos durante las sesiones PTZ	Seleccione la casilla de verificación para ocultar los nombres de los usuarios asociados a esta función cuando controlan sesiones PTZ.

Usuarios y grupos de la ficha (cometidos)

En la pestaña **Usuarios y grupos**, se asignan usuarios y grupos a los cometidos (ver "Asignar / eliminar usuarios y grupos a / desde los cometidos" en la página 231). Puede asignar usuarios y grupos de Windows o usuarios básicos (ver "Usuarios (explicado)" en la página 229).

Nombre	Descripción
Nombre	Muestra el nombre del usuario o grupo asignado a esta función.
Descripción	Muestra la descripción que introdujo cuando se creó el usuario básico.

Pestaña de Seguridad General (cometidos)

Funcionalidad disponible depende del sistema que está utilizando. Ver tabla de comparación de productos (en la página 24) para más información.

En la ficha **Seguridad general**, configura derechos generales para los cometidos. Para cada componente disponible en el sistema, decida si desea **Permitir** o **Denegar** usuarios con el cometido de los derechos para acceder y utilizar diferentes zonas en el componente correspondiente.

Nota: Los ajustes globales de seguridad sólo se aplican al sitio actual.

Se puede asociar un usuario con más de un cometido. Si selecciona **Denegar** en una configuración de seguridad para un cometido y **Permitir** para otro, el permiso **Denegar** derecho prevalece sobre el permiso **Permitir** derecho.

La ficha **Seguridad general** está disponible en todos los productos excepto en XProtect Essential+, pero la pestaña le ofrece la posibilidad de cambiar más funciones en XProtect Corporate que en XProtect Expert, XProtect Professional+ y XProtect Express+. Esto se debe a que solo puede configurar derechos de administrador diferenciados en XProtect Corporate, mientras que puede configurar derechos generales para un rol que use XProtect Smart Client, XProtect Web Client o Milestone Mobile cliente en todos los productos.

A continuación, las descripciones muestran lo que sucede en cada derecho individual para los diferentes componentes del sistema si selecciona **Permitir** para el cometido relevante. Si usa XProtect Corporate, puede ver qué configuraciones son **solo** disponibles para usted en cada componente del sistema.

Para cada componente o funcionalidad del sistema, el administrador del sistema completo puede utilizar las casillas de verificación **Permitir** o **Denegar** para configurar permisos de seguridad para el cometido. Los permisos de seguridad se configura aquí se establecen para todo el sistema o componente de funcionalidad. Por ejemplo, si selecciona la casilla de verificación **Denegar** en **Cámaras,** todas las cámaras agregadas al sistema no están disponibles para el cometido. Por el contrario, si selecciona la casilla de verificación **Permitir**, el cometido puede ver todas las cámaras añadidas al sistema. El resultado de la selección **Permitir** o **Denegar** en las cámaras es que la configuración de la cámara en la ficha **Dispositivo** heredar entonces sus selecciones en la pestaña **Seguridad general** para que todas las cámaras estén disponibles o no disponibles para el cometido en particular.

Si desea establecer permisos de seguridad para cámaras **individuales** o similares, sólo se puede establecer estos permisos individuales en la pestaña del componente o funcionalidad del sistema relevante si tiene **no establece los permisos globales** para el componente de sistema o funcionalidad en pestaña **Seguridad general**.

Las descripciones a continuación también se aplican a los derechos que puede configurar a través de los SDK de MIP.

Importante: Si cambia su licencia base de XProtect Corporate a uno de los otros productos, solo puede hacerlo si no ha establecido ningún derecho de seguridad para la función que no está disponible en esos productos. Por lo tanto, para completar un interruptor de este tipo, asegúrese de que se retiran todos los derechos de seguridad que están a la disposición de XProtect Corporate.

Servidor de gestión

Derecho de seguridad	Descripción	XProtect Corporate
Control total	Habilita el derecho de administrar todas las entradas de la seguridad en esta parte del sistema.	
Leer	Permite que el derecho a acceder a una amplia gama de funciones, incluyendo: • Inicio de sesión en el Management Client • Lista de tareas actuales • Los registros del servidor. También permite el acceso a las siguientes funciones: • Servicios de conexión remota • Perfiles Smart Client • Los perfiles de Management Client • Matrix • Perfiles temporales • Servidores registrados y API del servicio de registro • Servidores Enterprise.	Solo disponible

Derecho de seguridad	Descripción	XProtect Corporate
Editar	Habilita el derecho de modificar los datos en una amplia gama de funciones, incluyendo: • Opciones • Gestión de licencias. También permite a los usuarios crear, eliminar y editar las siguientes características: • Servicios de conexión remota • Grupos de dispositivos • Matrix • Perfiles temporales • Perfiles de notificación • Servidores registrados • Servidores Enterprise. **Nota**: Permite a la derecha para configurar los rangos de IP locales al configurar la red en el servidor de grabación.	Solo disponible
Monitor de sistema	Permite a la derecha para ver los datos del Monitor de sistema.	Solo disponible
API de estado	Permite que el derecho a realizar consultas sobre la API de estado ubicado en el servidor de grabación. Esto significa que el cometido de este derecho activada, tiene acceso a leer el estado de los artículos que se encuentran en el servidor de grabación.	
Gestionar jerarquía de sitios federados	Habilita el derecho de añadir y separar el sitio actual a otros sitios en una jerarquía de sitios federados. **Nota**: Si se establece este permiso a permitido solamente en el sitio secundario, el usuario puede separar el sitio desde el sitio principal.	Solo disponible
Respaldar su configuración	Permite a la derecha para crear copias de seguridad de la configuración del sistema utilizando la copia de seguridad del sistema / restaurar la funcionalidad.	Solo disponible
Autorizar usuarios	Habilita el derecho de autorizar a los usuarios cuando se les pregunta por una segunda entrada en XProtect Smart Client o Management Client. Se define si un cometido requiere la autorización de inicio de sesión en la ficha **Información**.	

Derecho de seguridad	Descripción	XProtect Corporate
Gestionar seguridad	Habilita el derecho de administrar los permisos para el servidor de gestión. También permite a los usuarios crear, eliminar y editar las siguientes características: • Cometidos • Usuarios básicos • Perfiles Smart Client • Los perfiles de Management Client.	Solo disponible

Servidores de grabación

Los siguientes ajustes sólo están disponibles en XProtect Corporate.

Derecho de seguridad	Descripción
Control total	Habilita el derecho de administrar todas las entradas de la seguridad en esta parte del sistema.
Editar	Habilita el derecho de editar las propiedades de los servidores de grabación, a excepción de los ajustes de configuración de red que requieren **Editar** a la derecha en el servidor de gestión.
Borrar	Permite que el derecho a eliminar los servidores de grabación. Para ello, también debe dar al usuario borrar los permisos en: • Grupo de seguridad de hardware Si ha añadido hardware para el servidor de grabación. **Nota**: Si alguno de los dispositivos en el servidor de grabación contiene bloqueos de evidencia, sólo se puede eliminar el servidor de grabación si no está en línea.
Gestionar hardware	Habilita el derecho de añadir hardwareen servidores de grabación.
Gestionar almacenamiento	Habilita el derecho de administrar los contenedores de almacenamiento en la grabación de servidor, que es crear, borrar, mover y recipientes de almacenamiento vacíos.
Autorizar servidor de grabación	Habilita el derecho de autorizar nuevos servidores de grabación.
Gestionar seguridad	Habilita el derecho de administrar los permisos de seguridad para los servidores de grabación.

Servidores failover

Los siguientes ajustes sólo están disponibles en XProtect Corporate.

Derecho de seguridad	Descripción
Control total	Habilita el derecho de administrar todas las entradas de la seguridad en esta parte del sistema.
Leer	Permite que el derecho de ver y servidores de acceso failover en el Management Client.
Editar	Permite a la derecha para crear, actualizar, borrar, mover, y activar/desactivar los servidores de conmutación por error en la Management Client.
Gestionar seguridad	Habilita el derecho de administrar los permisos de seguridad para los servidores failover.

Servidores Mobile

Los siguientes ajustes sólo están disponibles en XProtect Corporate.

Derecho de seguridad	Descripción
Control total	Habilita el derecho de administrar todas las entradas de la seguridad en esta parte del sistema.
Leer	Permite que el derecho de ver y acceder a los servidores Mobile en el Management Client.
Editar	Habilita el derecho de editar y eliminar servidores Mobile en el Management Client.
Gestionar seguridad	Habilita el derecho de administrar los permisos de seguridad para los servidores Mobile.
Crear	Habilita el derecho de añadir servidores Mobile para el sistema.

Hardware

Los siguientes ajustes sólo están disponibles en XProtect Corporate.

Derecho de seguridad	Descripción
Control total	Habilita el derecho de administrar todas las entradas de la seguridad en esta parte del sistema.
Editar	Habilita el derecho de editar propiedades en el hardware.
Borrar	Habilita el derecho de eliminar hardware. **Nota**: Si alguno de los dispositivos de hardware contiene bloqueos de evidencia, sólo se puede eliminar si el hardware del servidor de grabación no está en línea.
Gestionar seguridad	Habilita el derecho de administrar los permisos de seguridad para el hardware.

Derecho de seguridad	Descripción
Comandos del controlador	Permite el derecho de enviar comandos especiales a los controladores y por lo tanto controlar las características y la configuración en el propio dispositivo. **Nota**: Los comandos **del controlador** son para plug-ins especiales desarrollados MIP sólo en los clientes. No controla las tareas de configuración estándar.

Cámaras

Derecho de seguridad	Descripción	XProtect Corporate
Control total	Habilita el derecho de administrar todas las entradas de la seguridad en esta parte del sistema.	
Leer	Permite a la derecha para ver los dispositivos de la cámara en los clientes y el Management Client.	
Editar	Habilita el derecho de editar las propiedades de las cámaras del Management Client. También permite a los usuarios activar o desactivar una cámara.	Solo disponible
Visión en directo	Permite a la derecha para ver el video en directo de cámaras en los clientes y el Management Client.	
Reproducción	Habilita el derecho de reproducir vídeo grabado en las cámaras de todos los clientes.	
Recuperar grabaciones a distancia	Permite que el derecho a recuperar las grabaciones en los clientes de las cámaras en sitios remotos o de almacenajes de borde en las cámaras.	
Leer secuencias	Habilita el derecho de leer la información de la secuencia relacionada con, por ejemplo, el explorador de secuencia en los clientes.	
Búsqueda avanzada	Habilita el derecho a utilizar la función de búsqueda avanzada en los clientes.	
Exportación	Habilita el derecho a exportar las grabaciones de los clientes.	
Crear marcador	Permite que el derecho a crear marcadores en el vídeo grabado en directo y en los clientes.	
Leer marcadores	Permite que el derecho a buscar y leer detalles del marcador en los clientes.	
Editar marcadores	Habilita el derecho de editar los marcadores en los clientes.	
Eliminar marcadores	Habilita el derecho a eliminar los marcadores en los clientes.	
Crear y ampliar bloqueos de evidencias	Habilita el derecho de crear y extender bloqueos de evidencias en los clientes.	Solo disponible
Leer bloqueo de evidencias	Permite que el derecho a buscar y leer bloqueos de evidencias en los clientes.	Solo disponible

Derecho de seguridad	Descripción	XProtect Corporate
Eliminar y reducir bloqueos de evidencias	Habilita el derecho de eliminar o reducir bloqueos de evidencias en los clientes.	Solo disponible
Iniciar grabación manual	Permite a la derecha para iniciar la grabación manual de vídeo en los clientes.	
Detener la grabación manual	Habilita el derecho de detener la grabación manual de vídeo en los clientes.	
Comandos AUX	Habilita el derecho a utilizar los comandos auxiliares (AUX) en la cámara de los clientes. **Comandos AUX** ofrecen a los usuarios el control de, por ejemplo, limpiaparabrisas en una cámara conectada a través de un servidor de vídeo. Dispositivos con cámara y asociados conectados a través de conexiones auxiliares se controlan desde el cliente.	
PTZ manual	Habilita el derecho de usar funciones PTZ en cámaras PTZ en los clientes y el Management Client.	
Activar preajustes PTZ o perfil patrullando	Permite a la derecha para mover las cámaras PTZ a posiciones predeterminadas, iniciar y detener el patrullaje perfiles, y pausar un patrullaje en los clientes y el Management Client. Para permitir este cometido para utilizar otras funciones PTZ de la cámara, permitir la derecha **PTZ manual**.	
Gestionar valores preestablecidos PTZ o perfiles de patrulla	Permite que el derecho de añadir, editar y borrar los preajustes PTZ y perfiles de patrullaje de las cámaras PTZ en los clientes y el Management Client. Para permitir este cometido para utilizar otras funciones PTZ de la cámara, permitir la derecha **PTZ manual**.	
Bloquear/Desbloquear valores preestablecidos PTZ	Permite a la derecha para bloquear y desbloquear preajustes de PTZ en el Management Client. Esto impide o permite que otros usuarios cambien las posiciones predeterminadas en los clientes y en la Management Client.	Solo disponible
Reservar sesiones PTZ	Permite a la derecha para ajustar las cámaras PTZ en el modo PTZ sesión reservada en los clientes y el Management Client. En una sesión reservada PTZ otros usuarios con mayor prioridad PTZ no son capaces de asumir el control. Para permitir este cometido para utilizar otras funciones PTZ de la cámara, permitir la derecha **PTZ manual**.	Solo disponible
Lanzar peticiones PTZ	Permite a la derecha para liberar sesiones PTZ de otros usuarios del Management Client. Siempre se puede liberar sus propias sesiones de PTZ - sin este permiso.	Solo disponible
Borrar grabaciones	Habilita el derecho de borrar grabaciones de vídeo almacenados en el sistema a través de la Management Client.	Solo disponible

Derecho de seguridad	Descripción	XProtect Corporate
Levantar máscaras de privacidad	Permite el derecho de levantar temporalmente máscaras de privacidad en XProtect Smart Client. También habilita el derecho de autorizar a otros usuarios de XProtect Smart Client a levantar máscaras de privacidad. **Nota**: Las máscaras de privacidad de elevación solo se aplican a las máscaras de privacidad configuradas como máscaras de privacidad que se pueden subir en el Management Client.	
Gestionar seguridad	Habilita el derecho de administrar los permisos de seguridad en el Management Client para la cámara.	Solo disponible

Micrófonos

Derecho de seguridad	Descripción	XProtect Corporate
Control total	Habilita el derecho de administrar todas las entradas de la seguridad en esta parte del sistema.	
Leer	Permite a la derecha para ver los dispositivos de micrófono en los clientes y el Management Client.	
Editar	Habilita el derecho de editar las propiedades del micrófono en el Management Client. También permite a los usuarios activar o desactivar los micrófonos.	Solo disponible
Escuchar	Permite a la derecha para escuchar el audio en directo desde los micrófonos de los clientes y el Management Client.	
Reproducción	Permite que el derecho a reproducir el audio grabado de los micrófonos en los clientes.	
Recuperar grabaciones a distancia	Permite que el derecho a recuperar las grabaciones en los clientes de los micrófonos de los sitios remotos o de almacenajes de borde en las cámaras.	
Leer secuencias	Habilita el derecho de leer la información de la secuencia relacionada con, por ejemplo, el explorador de secuencia en los clientes.	
Exportación	Habilita el derecho a exportar las grabaciones de los clientes.	
Crear marcador	Permite que el derecho a crear marcadores en los clientes.	
Leer marcadores	Permite que el derecho a buscar y leer detalles del marcador en los clientes.	
Editar marcadores	Habilita el derecho de editar los marcadores en los clientes.	
Eliminar marcadores	Habilita el derecho a eliminar los marcadores en los clientes.	
Crear y ampliar bloqueos de evidencias	Permite que el derecho a crear o ampliar bloqueos de evidencias en los clientes.	Solo disponible

Derecho de seguridad	Descripción	XProtect Corporate
Leer bloqueo de evidencias	Permite que el derecho a buscar y leer los detalles del bloqueos de evidencias en los clientes.	Solo disponible
Eliminar y reducir bloqueos de evidencias	Habilita el derecho de eliminar o reducir bloqueos de evidencias en los clientes.	Solo disponible
Iniciar grabación manual	Permite a la derecha para iniciar la grabación manual de audio de los clientes.	
Detener la grabación manual	Habilita el derecho de detener la grabación manual de audio de los clientes.	
Borrar grabaciones	Habilita el derecho de borrar grabaciones almacenadas en el sistema.	Solo disponible
Gestionar seguridad	Habilita el derecho de administrar los permisos de seguridad en el Management Client para los micrófonos.	Solo disponible

Altavoces

Derecho de seguridad	Descripción	XProtect Corporate
Control total	Habilita el derecho de administrar todas las entradas de la seguridad en esta parte del sistema.	
Leer	Permite a la derecha para ver los dispositivos de altavoz de los clientes y el Management Client.	
Editar	Habilita el derecho de editar las propiedades de los altavoces del Management Client. También permite a los usuarios activar o desactivar los altavoces.	Solo disponible
Escuchar	Permite a la derecha para escuchar el audio en directo desde los altavoces de los clientes y el Management Client.	
Hablar	Permite que el derecho a hablar a través de los altavoces de los clientes.	
Reproducción	Permite que el derecho a reproducir el audio grabado desde los altavoces en los clientes.	
Recuperar grabaciones a distancia	Permite que el derecho a recuperar las grabaciones en los clientes de los altavoces en lugares remotos o de almacenajes de borde en las cámaras.	
Leer secuencias	Permite que el derecho de uso de las secuencias de función durante la navegación audio grabado desde los altavoces de los clientes.	
Exportación	Permite que el derecho a la exportación de audio grabado desde los altavoces de los clientes.	
Crear marcador	Permite que el derecho a crear marcadores en los clientes.	

Derecho de seguridad	Descripción	XProtect Corporate
Leer marcadores	Permite que el derecho a buscar y leer detalles del marcador en los clientes.	
Editar marcadores	Habilita el derecho de editar los marcadores en los clientes.	
Eliminar marcadores	Habilita el derecho a eliminar los marcadores en los clientes.	
Crear y ampliar bloqueos de evidencias	Permite que el derecho a crear o ampliar bloqueos de evidencia de audio grabado en los clientes.	Solo disponible
Leer bloqueo de evidencias	Permite a la derecha para ver bloqueos de evidencias de audio grabado en los clientes.	Solo disponible
Eliminar y reducir bloqueos de evidencias	Habilita el derecho de eliminar o reducir bloqueos de evidencias de audio grabado en los clientes.	Solo disponible
Iniciar grabación manual	Permite a la derecha para iniciar la grabación manual de audio de los clientes.	
Detener la grabación manual	Habilita el derecho de detener la grabación manual de audio de los clientes.	
Borrar grabaciones	Habilita el derecho de borrar grabaciones almacenadas en el sistema.	Solo disponible
Gestionar seguridad	Habilita el derecho de administrar los permisos de seguridad en el Management Client para los altavoces.	Solo disponible

Metadatos

Derecho de seguridad	Descripción	XProtect Corporate
Control total	Habilita el derecho de administrar todas las entradas de la seguridad en esta parte del sistema.	
Leer	Permite que el derecho a recibir los metadatos de los clientes.	
Editar	Habilita el derecho de editar las propiedades de metadatos en el Management Client. También permite a los usuarios activar o desactivar los dispositivos de metadatos.	Solo disponible
Directo	Permite que el derecho a recibir los metadatos en directo de cámaras en los clientes.	
Reproducción	Habilita el derecho de reproducir los datos desde dispositivos de metadatos en los clientes.	
Recuperar grabaciones a distancia	Permite que el derecho a recuperar las grabaciones en los clientes de dispositivos de metadatos en los sitios remotos o de almacenajes de borde en las cámaras.	
Leer secuencias	Habilita el derecho de leer la información de la secuencia relacionada con, por ejemplo, el explorador de secuencia en los clientes.	

Derecho de seguridad	Descripción	XProtect Corporate
Exportación	Habilita el derecho a exportar las grabaciones en los clientes.	
Crear y ampliar bloqueos de evidencias	Permite a la derecha para crear bloqueos de evidencias en los clientes.	Solo disponible
Leer bloqueo de evidencias	Permite a la derecha para ver bloqueos de evidencias en los clientes.	Solo disponible
Eliminar y reducir bloqueos de evidencias	Habilita el derecho de eliminar o reducir bloqueos de evidencias en los clientes.	Solo disponible
Iniciar grabación manual	Permite a la derecha para iniciar la grabación manual de los metadatos de los clientes.	
Detener la grabación manual	Habilita el derecho de detener la grabación manual de metadatos en los clientes.	
Borrar grabaciones	Habilita el derecho de borrar grabaciones almacenadas en el sistema.	Solo disponible
Gestionar seguridad	Habilita el derecho de administrar los permisos de seguridad en el Management Client para los metadatos.	Solo disponible

Entrada

Derecho de seguridad	Descripción	XProtect Corporate
Control total	Habilita el derecho de administrar todas las entradas de la seguridad en esta parte del sistema.	Solo disponible
Leer	Permite a la derecha para ver los dispositivos de entrada de los clientes y el Management Client.	
Editar	Habilita el derecho de editar las propiedades de los dispositivos de entrada del Management Client. También permite a los usuarios activar o desactivar un dispositivo de entrada.	Solo disponible
Gestionar seguridad	Habilita el derecho de administrar los permisos de seguridad en el Management Client para dispositivos de entrada.	Solo disponible

Salida

Derecho de seguridad	Descripción	XProtect Corporate
Control total	Habilita el derecho de administrar todas las entradas de la seguridad en esta parte del sistema.	
Leer	Permite a la derecha para ver los dispositivos de salida de los clientes.	

Derecho de seguridad	Descripción	XProtect Corporate
Editar	Habilita el derecho de editar las propiedades de los dispositivos de salida del Management Client. También permite a los usuarios activar o desactivar un dispositivo de salida.	Solo disponible
Activar	Permite a la derecha para activar las salidas de los clientes.	
Gestionar seguridad	Habilita el derecho de administrar los permisos de seguridad en el Management Client para dispositivos de salida.	Solo disponible

Smart Wall

La siguiente configuración solo está disponible en XProtect Expert y XProtect Corporate.

Derecho de seguridad	Descripción	XProtect Corporate
Control total	Habilita el derecho de administrar todas las entradas de la seguridad en esta parte del sistema.	
Leer	Permite a la derecha para ver las Smart Walls en los clientes.	
Editar	Habilita el derecho de editar las propiedades para el Smart Wall en el Management Client.	Solo disponible
Borrar	Habilita el derecho de eliminar Smart Walls existentes en el Management Client.	Solo disponible
Operación	Permite a la derecha para activar y modificar Smart Walls, por ejemplo para cambiar y activar o aplicar ajustes preestablecidos de cámaras en puntos de vista en los clientes y en la Management Client.	
Crear Smart Wall	Habilita el derecho de crear nuevos Smart Walls en el Management Client.	Solo disponible
Gestionar seguridad	Habilita el derecho de administrar los permisos de seguridad en el Management Client para la Smart Wall.	Solo disponible
Reproducción	Permite el derecho a reproducir datos grabados desde dentro de Smart Wall s en los clientes.	

Grupos de vistas

Derecho de seguridad	Descripción	XProtect Corporate
Control total	Habilita el derecho de administrar todas las entradas de la seguridad en esta parte del sistema.	
Leer	Permite a la derecha para ver grupos de vistas en los clientes y en el Management Client. Grupos de vistas se crean en el Management Client.	
Editar	Habilita el derecho de editar las propiedades de los Grupos de vistas en el Management Client.	Solo disponible
Borrar	Habilita el derecho de eliminar grupos de vistas en el Management Client.	
Operación	Permite el derecho a utilizar grupos de vistas en XProtect Smart Client, esto es para crear y eliminar subgrupos y vistas.	
Crear grupo de vistas	Permite a la derecha para crear grupos de vistas en el Management Client.	Solo disponible
Gestionar seguridad	Habilita el derecho de administrar los permisos de seguridad en el Management Client para grupos de vistas.	Solo disponible

Eventos definidos por el usuario

Derecho de seguridad	Descripción	XProtect Corporate
Control total	Habilita el derecho de administrar todas las entradas de la seguridad en esta parte del sistema.	
Leer	Permite a la derecha para ver los eventos definidos por el usuario en los clientes.	
Editar	Habilita el derecho de editar las propiedades de eventos definidos por el usuario del Management Client.	Solo disponible
Borrar	Permite que el derecho a eliminar los eventos definidos por el usuario en el Management Client.	Solo disponible
Activador	Permite a la derecha para activar eventos definidos por el usuario en los clientes.	
Gestionar seguridad	Habilita el derecho de administrar los permisos de seguridad en el Management Client para eventos definidos por el usuario.	Solo disponible
Crear evento definido por el usuario	Permite que el derecho a crear nuevos eventos definidos por el usuario del Management Client.	Solo disponible

Eventos Genéricos

Los siguientes ajustes sólo están disponibles en XProtect Corporate.

Derecho de seguridad	Descripción
Control total	Habilita el derecho de administrar todas las entradas de la seguridad en esta parte del sistema.
Leer	Permite a la derecha para ver los eventos genéricos en los clientes y el Management Client.
Editar	Habilita el derecho de editar las propiedades de eventos genéricos del Management Client.
Borrar	Permite que el derecho a eliminar los eventos genéricos en el Management Client.
Gestionar seguridad	Habilita el derecho de administrar los permisos de seguridad en el Management Client para eventos genéricos.
Crear	Permite que el derecho a crear nuevos eventos genéricos del Management Client.

Eventos analíticos

Los siguientes ajustes sólo están disponibles en XProtect Corporate.

Derecho de seguridad	Descripción
Control total	Habilita el derecho de administrar todas las entradas de la seguridad en esta parte del sistema.
Leer	Permite a la derecha para ver los eventos de analytics en el Management Client.
Editar	Habilita el derecho de editar las propiedades de eventos analíticos del Management Client.
Borrar	Permite que el derecho a eliminar los eventos de análisis en el Management Client.
Crear	Permite que el derecho a crear nuevos evento de analytics del Management Client.
Gestionar seguridad	Habilita el derecho de administrar los permisos de seguridad en el Management Client para los eventos analíticos.

Matrix

Derecho de seguridad	Descripción	XProtect Corporate
Control total	Habilita el derecho de administrar todas las entradas de la seguridad en esta parte del sistema.	Solo disponible
Leer	Permite que el derecho de seleccionar y enviar vídeo al destinatario Matrix de los clientes.	
Editar	Activa el derecho de editar las propiedades de los Matrix en el Management Client.	Solo disponible
Borrar	Habilita el derecho de eliminar Matrix 's en el Management Client.	Solo disponible
Crear Matrix	Habilita el derecho de crear nuevos Matrix 's en el Management Client.	Solo disponible
Gestionar seguridad	Habilita el derecho de administrar los permisos de seguridad en el Management Client para todos Matrixs.	Solo disponible

Reglas

Los siguientes ajustes sólo están disponibles en XProtect Corporate.

Derecho de seguridad	Descripción
Control total	Habilita el derecho de administrar todas las entradas de la seguridad en esta parte del sistema.
Leer	Permite a la derecha para ver las reglas existentes en el Management Client.
Editar	Habilita el derecho de editar propiedades de las reglas y la regla para definir el comportamiento del Management Client. También requiere que el usuario tiene permisos de lectura en todos los dispositivos que se ven afectados por la regla.
Borrar	Permite que el derecho a eliminar las reglas del Management Client. También requiere que el usuario tiene permisos de lectura en todos los dispositivos que se ven afectados por la regla.
Crear regla	Permite que el derecho a crear nuevas reglas en el Management Client. También requiere que el usuario tiene permisos de lectura en todos los dispositivos que se ven afectados por la regla.
Gestionar seguridad	Habilita el derecho de administrar los permisos de seguridad en el Management Client para todas las reglas.

Sitios

Los siguientes ajustes sólo están disponibles en XProtect Corporate.

Derecho de seguridad	Descripción
Control total	Habilita el derecho de administrar todas las entradas de la seguridad en esta parte del sistema.
Leer	Permite a la derecha para ver otros sitios del Management Client. Sitios conectados están conectados a través de Milestone Federated Architecture. Para editar las propiedades, necesita permisos de edición en el servidor de gestión en cada sitio.
Gestionar seguridad	Habilita el derecho de administrar los permisos de seguridad todos los sitios.

Alarmas

Los siguientes ajustes sólo están disponibles en XProtect Corporate.

Derecho de seguridad	Descripción
Control total	Habilita el derecho de administrar todas las entradas de la seguridad en esta parte del sistema.
Leer	Permite a la derecha para ver las definiciones de alarma, suena la alarma, y la configuración de datos de alarma en el Management Client. **Nota**: Sólo cuando establece esto como permitido, aparece la pestaña **Alarmas y eventos** en el cuadro de diálogo **Opciones**.
Editar	Habilita el derecho de editar las propiedades de las definiciones de alarma, suena la alarma y la configuración de datos de alarma del Management Client.
Borrar	Permite que el derecho a eliminar definiciones de alarma en el Management Client.
Gestionar seguridad	Habilita el derecho de administrar los permisos de seguridad para las alarmas.
Crear	Permite a la derecha para crear nuevas definiciones de alarma en el Management Client.

Control de acceso

Los siguientes ajustes sólo están disponibles en XProtect Corporate.

Derecho de seguridad	Descripción
Control total	Habilita el derecho de administrar todas las entradas de la seguridad en esta parte del sistema.
Leer	Permite a la derecha para ver las propiedades de los sistemas de control de acceso del Management Client.
Editar	Habilita el derecho de editar las propiedades de los sistemas de control de acceso del Management Client.

Derecho de seguridad	Descripción
Borrar	Habilita el derecho de eliminar los sistemas de control de acceso del Management Client.
Crear	Habilita el derecho de crear nuevos sistemas de control de acceso del Management Client.
Gestionar seguridad	Habilita el derecho de administrar los permisos de seguridad para todos los sistemas de control de acceso.

Monitores del sistema

La siguiente configuración solo está disponible en XProtect Expert y XProtect Corporate.

Derecho de seguridad	Descripción
Control total	Habilita el derecho de administrar todas las entradas de la seguridad en esta parte del sistema.
Leer	Permite a la derecha para ver los monitores de sistema en XProtect Smart Client.
Editar	Habilita el derecho de editar las propiedades de los monitores del sistema en el Management Client.
Gestionar seguridad	Habilita el derecho de administrar los permisos de seguridad en el Management Client para todos los monitores de sistema.

Fuentes de la transacción

Derecho de seguridad	Descripción
Control total	Habilita el derecho de administrar todas las entradas de la seguridad en esta parte del sistema.
Leer	Permite a la derecha para ver las propiedades de las fuentes de transacción en el Management Client.
Editar	Habilita el derecho de editar las propiedades de las fuentes de transacción en el Management Client.
Borrar	Habilita el derecho de eliminar las fuentes de transacción en el Management Client.
Crear	Permite a la derecha para crear nuevas fuentes de transacción en el Management Client.
Gestionar seguridad	Habilita el derecho de administrar los permisos de seguridad en el Management Client para todas las fuentes de transacción.

Las definiciones de transacción

Derecho de seguridad	Descripción
Control total	Habilita el derecho de administrar todas las entradas de la seguridad en esta parte del sistema.
Leer	Permite a la derecha para ver las propiedades de las definiciones de transacción en el Management Client.
Editar	Habilita el derecho de editar las propiedades de las definiciones de transacción en el Management Client.
Borrar	Permite que el derecho a eliminar definiciones de transacción en el Management Client.
Crear	Permite a la derecha para crear nuevas definiciones de transacción en el Management Client.
Gestionar seguridad	Habilita el derecho de administrar los permisos de seguridad en el Management Client para todas las definiciones de transacción.

Pestaña Dispositivo (cometidos)

Funcionalidad disponible depende del sistema que está utilizando. Ver tabla de comparación de productos (en la página 24) para más información.

La ficha **Dispositivo** le permite especificar qué características pueden utilizar los usuarios / grupos con la función seleccionada para cada dispositivo (por ejemplo, una cámara) o grupo de dispositivos en XProtect Smart Client.

Recuerde que debe repetir para cada dispositivo. También puede seleccionar un grupo de dispositivos, y especificar los derechos de cometidos para todos los dispositivos del grupo de una sola vez.

Todavía puede seleccionar o eliminar estas casillas de verificación cuadradas, pero tenga en cuenta que su elección en este caso se aplica a **todos los dispositivos** dentro del grupo de dispositivos. Como alternativa, seleccione los dispositivos individuales en el grupo de dispositivos para verificar exactamente qué dispositivos de la derecha relevante se opte.

Los derechos relacionados con la cámara

Especificar los siguientes derechos para los dispositivos de la cámara:

Nombre	Descripción
Leer	La cámara (s) seleccionado será visible en los clientes.
Visión en directo	Permite la visualización en directo de vídeo de la cámara (s) seleccionado en los clientes. Para XProtect Smart Client, se requiere que el cometido se haya concedido el derecho de ver la ficha **Directo** de los clientes. Este derecho se concede como parte de los derechos de la aplicación. Especificar el perfil temporal o deje el valor predeterminado.
Reproducción> Dentro de perfil temporal	Permite la reproducción de vídeo grabado por la cámara (s) seleccionado en los clientes. Especificar el perfil temporal o deje el valor predeterminado.

Nombre	Descripción
Reproducción> Limitar la reproducción para	Permite la reproducción de vídeo grabado por la cámara (s) seleccionado en los clientes. Especificar un límite de reproducción o aplicar ninguna restricción.
Leer secuencias	Permite la lectura de la información de la secuencia relacionada con, por ejemplo, el explorador de secuencia en los clientes.
Búsqueda avanzada	Permite al usuario utilizar la función de búsqueda avanzada en los clientes.
Exportación	Permite al usuario exportar las grabaciones de los clientes.
Iniciar grabación manual	Permite iniciar la grabación manual de vídeo de la cámara (s) seleccionado en los clientes.
Detener la grabación manual	Permite detener la grabación manual de vídeo de la cámara (s) seleccionado en los clientes.
Leer marcadores	Permite buscar y leer detalles del marcador en los clientes.
Editar marcadores	Permite la edición de marcadores en los clientes.
Crear marcador	Permite añadir los marcadores en los clientes.
Eliminar marcadores	Permite borrar los marcadores en los clientes.
Comandos AUX	Permite el uso de comandos auxiliares de los clientes.
Crear y ampliar bloqueos de evidencias	Permite al usuario del cliente: • Añadir la cámara a nuevos o existentes bloqueos de evidencia. • Extender el tiempo de caducidad para bloqueos de evidencias existentes. • Extienda el intervalo protegido para bloqueos de evidencias existentes. Requiere derechos de usuario a todos los dispositivos incluidos en bloqueo de evidencia.
Eliminar y reducir bloqueos de evidencias	Permite al usuario del cliente: • Retire la cámara de bloqueos de evidencia existentes. • Eliminar bloqueos de evidencias existentes. • Acortar el tiempo de caducidad para bloqueos de evidencias existentes. • Reduzca el intervalo protegido para bloqueos de evidencias existentes. Requiere derechos de usuario a todos los dispositivos incluidos en bloqueo de evidencia.
Leer bloqueo de evidencias	Permite al usuario del cliente para buscar y leer los detalles del bloqueo en la evidencia.

Los derechos relacionados con micrófono

Especificar los siguientes derechos para los dispositivos de micrófono:

Nombre	Descripción
Leer	El micrófono (s) seleccionado será visible en los clientes.
Vivir> Escuchar	Permite escuchar audio en directo desde los micrófonos (s) seleccionados en los clientes. Para XProtect Smart Client, se requiere que el cometido se haya concedido el derecho de ver los clientes **Directo** pestaña. Este derecho se concede como parte de los derechos de la aplicación. Especificar el perfil temporal o deje el valor predeterminado.
Reproducción> Dentro de perfil temporal	Permite la reproducción de audio grabado desde el micrófono (s) seleccionado en los clientes. Especificar el perfil temporal o deje el valor predeterminado.
Reproducción> Limitar la reproducción para	Permite la reproducción de audio grabado desde el micrófono (s) seleccionado en los clientes. Especificar un límite de reproducción o aplicar ninguna restricción.
Leer secuencias	Permite la lectura de la información de la secuencia relacionada con, por ejemplo, el explorador de secuencia en los clientes.
Exportación	Permite al usuario exportar las grabaciones de los clientes.
Iniciar grabación manual	Permite iniciar la grabación manual de audio desde el micrófono (s) seleccionado en los clientes.
Detener la grabación manual	Permite detener la grabación manual de audio desde el micrófono (s) seleccionado en los clientes.
Leer marcadores	Permite buscar y leer detalles del marcador en los clientes.
Editar marcadores	Permite la edición de marcadores en los clientes.
Crear marcador	Permite añadir los marcadores en los clientes.
Eliminar marcadores	Permite borrar los marcadores en los clientes.
Crear y ampliar bloqueos de evidencias	Permite al usuario del cliente: • Añadir el micrófono a nuevas o existentes bloqueos de evidencia. • Extender el tiempo de caducidad para bloqueos de evidencias existentes. • Extienda el intervalo protegido para bloqueos de evidencias existentes. Requiere derechos de usuario a todos los dispositivos incluidos en bloqueo de evidencia.

Nombre	Descripción
Eliminar y reducir bloqueos de evidencias	Permite al usuario del cliente: • Retire el micrófono de bloqueos de evidencias existentes. • Eliminar bloqueos de evidencias existentes. • Acortar el tiempo de caducidad para bloqueos de evidencias existentes. • Reduzca el intervalo protegido para bloqueos de evidencias existentes. Requiere derechos de usuario a todos los dispositivos incluidos en bloqueo de evidencia.
Leer bloqueo de evidencias	Permite al usuario del cliente para buscar y leer los detalles del bloqueo en la evidencia.

Los derechos relacionados con los altavoces

Especificar los siguientes derechos para los dispositivos de altavoz:

Nombre	Descripción
Leer	El altavoz (s) seleccionado es visible en los clientes.
Vivir> Escuchar	Permite escuchar en vivo el sonido del altavoz seleccionado (s) en los clientes. Para XProtect Smart Client, se requiere que el cometido se haya concedido el derecho de ver los clientes **Directo** pestaña. Este derecho se concede como parte de los derechos de la aplicación. Especificar el perfil temporal o deje el valor predeterminado.
Reproducción> Dentro de perfil temporal	Permite la reproducción de audio grabado desde el altavoz (s) seleccionado en los clientes. Especificar el perfil temporal o deje el valor predeterminado.
Reproducción> Limitar la reproducción para	Permite la reproducción de audio grabado desde el altavoz (s) seleccionado en los clientes. Especificar un límite de reproducción o aplicar ninguna restricción.
Leer secuencias	Permite la lectura de la información de la secuencia relacionada con, por ejemplo, el explorador de secuencia en los clientes.
Exportación	Permite al usuario exportar las grabaciones de los clientes.
Iniciar grabación manual	Permite iniciar la grabación manual de audio del altavoz seleccionado (s) en los clientes.
Detener la grabación manual	Permite detener la grabación manual de audio del altavoz seleccionado (s) en los clientes.
Leer marcadores	Permite buscar y leer detalles del marcador en los clientes.
Editar marcadores	Permite la edición de marcadores en los clientes.

Nombre	Descripción
Crear marcador	Permite añadir los marcadores en los clientes.
Eliminar marcadores	Permite borrar los marcadores en los clientes.
Crear y ampliar bloqueos de evidencias	Permite al usuario del cliente: • Añadir el altavoz a nuevos o bloqueos de evidencias existentes. • Extender el tiempo de caducidad para bloqueos de evidencias existentes. • Extienda el intervalo protegido para bloqueos de evidencias existentes. Requiere derechos de usuario a todos los dispositivos incluidos en bloqueo de evidencia.
Eliminar y reducir bloqueos de evidencias	Permite al usuario del cliente: • Retire el altavoz de bloqueos de evidencia existentes. • Eliminar bloqueos de evidencias existentes. • Acortar el tiempo de caducidad para bloqueos de evidencias existentes. • Reduzca el intervalo protegido para bloqueos de evidencias existentes. Requiere derechos de usuario a todos los dispositivos incluidos en bloqueo de evidencia.
Leer bloqueo de evidencias	Permite al usuario del cliente para buscar y leer los detalles del bloqueo en la evidencia.

Los derechos relacionados con metadatos

Especificar los siguientes derechos para los dispositivos de metadatos:

Nombre	Descripción
Leer	Permite a la derecha para ver los dispositivos de metadatos y recuperar datos de ellos en los clientes.
Editar	Habilita el derecho de editar las propiedades de metadatos. También permite a los usuarios activar o desactivar los dispositivos de metadatos en el Management Client ya través del MIP SDK.
Visión en directo	Permite a la derecha para ver los metadatos de las cámaras en los clientes. Para XProtect Smart Client, se requiere que el cometido se haya concedido el derecho de ver la ficha **Directo** de los clientes. Este derecho se concede como parte de los derechos de la aplicación.
Reproducción	Habilita el derecho de reproducir los datos desde dispositivos de metadatos en los clientes.

Nombre	Descripción
Leer secuencias	Permite que el derecho de uso de las secuencias de función durante la navegación por los datos registrados a partir de dispositivos de metadatos en los clientes.
Exportación	Permite que el derecho a la exportación de audio grabado desde dispositivos de metadatos en los clientes.
Crear y ampliar bloqueos de evidencias	Permite que el derecho a crear y ampliar las bloqueos de evidencias sobre los metadatos de los clientes.
Leer bloqueo de evidencias	Permite a la derecha para ver bloqueos de evidencias de metadatos en los clientes.
Eliminar y reducir bloqueos de evidencias	Habilita el derecho de eliminar o reducir bloqueos de evidencias de metadatos en los clientes.
Iniciar grabación manual	Permite a la derecha para iniciar la grabación manual de los metadatos de los clientes.
Detener la grabación manual	Habilita el derecho de detener la grabación manual de metadatos en los clientes.

Los derechos relacionados con la entrada

Especificar los siguientes derechos para los dispositivos de entrada:

Nombre	Descripción
Leer	Las entradas seleccionadas serán visibles en los clientes.

Los derechos relacionados con la producción

Especificar los siguientes derechos para los dispositivos de salida:

Nombre	Descripción
Leer	La salida (s) seleccionado será visible en los clientes. Si está visible, la salida será seleccionable en una lista de los clientes.
Activar	La salida seleccionada(s) se puede activar desde el Management Client y los clientes. Especificar el perfil temporal o deje el valor predeterminado.

Pestaña PTZ (cometidos)

Configure los derechos de las cámaras de zoom panorámico (PTZ) en la pestaña **PTZ**. Puede especificar las características de los usuarios / grupos pueden utilizar en los clientes. Puede seleccionar las cámaras PTZ individuales o grupos de dispositivos que contienen las cámaras PTZ.

Especificar los siguientes derechos para PTZ:

Nombre	Descripción
PTZ manual	Determina si el cometido seleccionada puede utilizar las funciones PTZ y pausar un patrullaje en la cámara seleccionada. Especificar un perfil temporal, seleccione **Siempre**, o deje el valor por defecto que sigue el perfil temporal predeterminado definido en la pestaña **Información** para ese cometido.
Activar valores preestablecidos PTZ o perfiles de patrulla	Determina si la función seleccionada se puede mover la cámara seleccionada a posiciones predeterminadas, iniciar y detener el patrullaje perfiles, y hacer una pausa en el patrullaje. Especificar un perfil temporal, seleccione **Siempre**, o deje el valor por defecto que sigue el perfil temporal predeterminado definido en la pestaña **Información** para ese cometido. Para permitir este cometido para utilizar otras funciones PTZ de la cámara, permitir la derecha **PTZ manual**.
Prioridad de PTZ	Determina la prioridad de las cámaras PTZ. Cuando varios usuarios en un sistema de vigilancia quieren controlar la misma cámara PTZ, al mismo tiempo, pueden producirse conflictos. Puede evitar esta situación mediante la especificación de una prioridad para el uso de la cámara PTZ seleccionado (s) por los usuarios / grupos con la función seleccionada. Especificar una prioridad de 1 a 32. 000, donde 1 es la prioridad más baja. La prioridad por defecto es 3. 000. El cometido con el número de prioridad más alta es el único que puede controlar la cámara (s) PTZ.
Gestionar valores preestablecidos PTZ o perfiles de patrulla	Determina el derecho de añadir, editar y borrar los preajustes PTZ y perfiles que patrullan en la cámara seleccionada, tanto en el Management Client y el XProtect Smart Client. Para permitir este cometido para utilizar otras funciones PTZ de la cámara, permitir la derecha **PTZ manual**.
Bloquear/Desbloquear valores preestablecidos PTZ	Determina si el cometido se puede bloquear y desbloquear posiciones preestablecidas de la cámara seleccionada.
Reservar sesiones PTZ	Determina la derecha para establecer la cámara seleccionada en el modo PTZ sesión reservada. En una sesión reservada PTZ otros usuarios o sesiones que patrullan con mayor prioridad PTZ no son capaces de asumir el control. Para permitir este cometido para utilizar otras funciones PTZ de la cámara, permitir la derecha **PTZ manual**.
Lanzar peticiones PTZ	Determina si el cometido seleccionado se puede liberar sesiones PTZ de otros usuarios del Management Client. Siempre se puede liberar sus propias sesiones de PTZ - sin este permiso.

Pestaña del habla (cometidos)

Relevante sólo si utiliza altavoces en su sistema. Especificar los siguientes derechos para los altavoces:

Nombre	Descripción
Hablar	Determinar si los usuarios se les debe permitir hablar a través del altavoz (s) seleccionado. Especificar el perfil temporal o deje el valor predeterminado.
Prioridad de habla	Cuando varios usuarios de los clientes quieren hablar a través del mismo orador, al mismo tiempo, pueden producirse conflictos. Resolver el problema especificando una prioridad para el uso de la bocina (s) seleccionados por los usuarios / grupos con la función seleccionada. Especifique una prioridad de **Muy bajo** a **Muy alto**. Se deja que el cometido de la más alta prioridad utilizar el altavoz antes de otros cometidos. En caso de que dos usuarios con el mismo cometido que desee hablar al mismo tiempo, el primer llegado, primer servido aplica en principios.

Pestaña Grabaciones remoto (cometidos)

Especificar los siguientes derechos para grabaciones remotas:

Nombre	Descripción
Recuperar grabaciones a distancia	Permite que el derecho a recuperar las grabaciones en los clientes de las cámaras, micrófonos, altavoces y dispositivos de metadatos en los sitios remotos o de almacenajes de borde en las cámaras.

Pestaña Smart Wall (cometidos)

A través de los cometidos, puede conceder sus derechos de usuario relacionados con la pared usuarios de Smart Client para la función Smart Wall:

Nombre	Descripción
Leer	Permite a los usuarios ver el Smart Wall seleccionado en los clientes.
Editar	Permite a los usuarios editar el Smart Wall seleccionado en el Management Client.
Borrar	Permite a los usuarios eliminar la Smart Wall seleccionado en el Management Client.
Operación	Permite a los usuarios aplicar diseños en la Smart Wall seleccionado en el cliente y para activar el preset seleccionado.
Reproducción	Permite a los usuarios reproducir datos grabados desde el Smart Wall seleccionado en los clientes.

Pestaña evento externo (cometidos)

Especificar los siguientes derechos de eventos externos:

Nombre	Descripción
Leer	Permite a los usuarios buscar y ver los eventos del sistema externo seleccionado en los clientes y el Management Client.
Editar	Permite a los usuarios editar el evento del sistema externo seleccionado en el Management Client.
Borrar	Permite a los usuarios eliminar el evento del sistema externo seleccionado en el Management Client.
Activador	Permite a los usuarios desencadenar el evento del sistema externo seleccionado en los clientes.

Pestaña grupo de vistas (cometidos)

En la pestaña **grupo de vistas**, se especifica qué grupos de vistas los usuarios y grupos de usuarios con la función seleccionada pueden utilizar en los clientes.

Especificar los siguientes derechos para los grupos de vistas:

Nombre	Descripción
Leer	Permite a la derecha para ver los grupos de vistas en los clientes y en el Management Client. Grupos de vistas se crean en el Management Client.
Editar	Habilita el derecho de editar propiedades en grupos de vistas en el Management Client.
Borrar	Habilita el derecho de eliminar grupos de vistas en el Management Client.
Operación	Permite el derecho a utilizar grupos de vistas en XProtect Smart Client, esto es para crear y eliminar subgrupos y vistas.

Pestaña Servidores (cometidos)

Especificar derechos de cometido en la pestaña **Servidores** sólo es relevante si ha integrado servidores XProtect Professional VMS en su sistema o su sistema funciona en una configuración de Milestone Federated Architecture.

Nombre	Descripción
Servidores Enterprise	Cuenta de usuario que proporciona acceso al servidor XProtect Professional VMS seleccionado. El usuario debe estar configurado en el servidor XProtect Professional VMS.
Sitios	Permite a la derecha para ver el sitio seleccionado en el Management Client. Sitios conectados están conectados a través de Milestone Federated Architecture. Para editar las propiedades, necesita permisos de edición en el servidor de gestión en cada sitio.

Ver servidores XProtect Professional VMS (explicado) (ver "Servidores XProtect Professional VMS (explicados)" en la página 440) o Milestone Federated Architecture (explicado) (en la página 298) para obtener más información.

Pestaña Matrix (cometidos)

Si ha configurado destinatarios de Matrix en su sistema, es posible configurar la derechos de cometidos Matrix. Desde un cliente, puede enviar vídeo a los destinatarios seleccionados Matrix. Seleccione los usuarios que pueden recibir esto en la pestaña Matrix.

Los siguientes derechos están disponibles:

Nombre	Descripción
Leer	Determinar si los usuarios y grupos con la función seleccionada pueden seleccionar y enviar vídeo al destinatario Matrix de los clientes.

Pestaña Alarmas (cometidos)

Si utiliza las alarmas en la configuración de su sistema para proporcionar información general y un control central de la instalación (incluyendo cualquier otro XProtect servidores), puede utilizar los **Alarmas** ficha para especificar los usuarios de derechos de alarma / grupos con el cometido seleccionado debe tener, por ejemplo, cómo manejar las alarmas en los clientes.

Especificar los siguientes derechos para las alarmas:

Nombre	Descripción
Gestionar	Permite que el derecho a gestionar las alarmas, por ejemplo, cambios en las prioridades de las alarmas y alarmas re-delegado a otros usuarios, reconocer las alarmas y cambiar el estado, por ejemplo, de **Nueva** a **Asignado**, de varias alarmas al mismo tiempo.
Vista	Permite a la derecha para ver las alarmas e informes de alarma de impresión.
Desactivar las alarmas	Permite que el derecho a desactivar las alarmas.
Recibir notificaciones	Permite que el derecho a recibir notificaciones acerca de las alarmas en los clientes.

Pestaña Control de acceso (cometidos)

Al añadir o editar usuarios básicos, usuarios o grupos de Windows, especifique la configuración de control de acceso:

Nombre	Descripción
Usar control de acceso	Permite al usuario utilizar las funciones relacionadas con el control de acceso en los clientes.
Ir al listado de titulares de tarjetas	Permite al usuario ver la lista de titulares de tarjetas en la pestaña **Control de Acceso** en los clientes.
Recibir notificaciones	Permite al usuario recibir notificaciones sobre solicitudes de acceso en los clientes.

LPR ficha (cometidos)

Si el sistema se ejecuta con XProtect LPR, especifique los siguientes derechos para los usuarios:

Nombre	Descripción
Utilizar LPR	Permite el derecho a utilizar cualquier característica relacionada con LPR en los clientes.
Gestionar listas de coincidencia de matrículas	Habilita el derecho de añadir, importar, modificar, exportar y eliminar las listas de coincidencia de matrículas en el Management Client.
Leer las listas de coincidencia de matrículas	Permite a la derecha para ver las listas de coincidencia de matrículas.

MIP ficha (funciones)

A través del MIP Software Development Kit (SDK), un proveedor externo puede desarrollar complementos personalizados para su sistema, por ejemplo, integración con sistemas de control de acceso externos o una funcionalidad similar.

¿Qué valores que se modifican para su plug-in de depender del plug-in correspondiente. Busque la configuración personalizada de los complementos en la ficha **MIP**.

Usuarios básicos

Usuarios básicos (explicado)

Cuando se agrega un usuario básico de su sistema, se crea una cuenta de usuario del sistema de vigilancia específica con el nombre de usuario básica y autenticación de contraseña para el usuario individual. Esto está en contraste con el usuario de Windows, añadido a través de Active Directory.

Cuando se trabaja con los usuarios básicos, es importante entender la diferencia entre el usuario y la base de usuario de Windows.

- Los usuarios básicos se autentican mediante una combinación de nombre de usuario / contraseña y son específicos de un sistema. Incluso si los usuarios básicos tienen el mismo nombre y contraseña, un usuario básico creado en un sitio federado no tienen acceso a otro sitio federado.
- Los usuarios de Windows son autenticados en función de su inicio de sesión de Windows y son específicos de una máquina.

Crear usuarios básicos

Para crear un usuario básico en el sistema:

1. Expandir **Seguridad** > **Usuarios básicos**.
2. En los **usuarios básicos** panel, haga clic derecho y seleccione **Crear usuario básico**.
3. Especificar un nombre de usuario y una contraseña, y repetirlo para asegurarse de que ha especificado correctamente.

4. Haga clic en **OK** para crear el usuario básico.

Panel de sistema

Panel de control del sistema (explicado)

Panel de sistema le proporciona la funcionalidad para supervisar el sistema y sus componentes.

Acceder a las siguientes funciones:

Nombre	Descripción
Monitor de sistema	Supervisar el estado de los servidores y las cámaras por los parámetros que defina.
Umbrales del monitor del sistema	Los valores umbral establecidos para los parámetros estudiados en los azulejos del servidor y del monitor utilizados en Monitor de sistema.
Bloqueo de evidencias	Obtener una visión general de todos los datos protegidos en el sistema.
Tarea actual	Obtener una visión general de las tareas en curso en el servidor de grabación seleccionado.
Informes de configuración	Decidir qué incluir en sus informes de configuración del sistema antes de imprimir.

Monitor del sistema (explicado)

Monitor del sistema le proporciona una visión general rápida, visual del estado actual de los servidores y las cámaras de su sistema a través de azulejos de colores que representan el hardware del sistema. Por defecto, el sistema muestra los azulejos que representan a todos los **servidores de grabación**, **Todos los servidores** y **todas las cámaras**.

El color de las fichas:

El color del azulejo	Descripción
Verde	Estado **Normal**. Todo funciona correctamente.
Amarillo	Estado **Advertencia**. Uno o más de los parámetros de monitorización está por encima del valor límite establecido (ver "Umbrales del monitor del sistema (explicados)" en la página 265) para el estado **Normal**.
Rojo	Estado **Crítico**. Uno o más de los parámetros de monitorización está por encima del valor límite establecido para el estado **Normal** y el estado de **Alerta**.

Puede personalizar las baldosas del servidor y de la cámara si desea mostrar más o menos fichas en el tablero de instrumentos. Por ejemplo, puede configurar los azulejos para representar un único servidor, una sola cámara, un grupo de cámaras, o un grupo de servidores. También puede eliminar un azulejo si no quiere usarlo

o editar sus parámetros de supervisión. Parámetros de control son, por ejemplo, uso de la CPU o la memoria disponible para un servidor. Si elimina estos parámetros desde el servidor de baldosas, la baldosa no supervisa estos parámetros en el azulejo relevante. Haga clic en **Personalizar** en la esquina superior derecha de la ficha para abrir la ventana Personalizar el panel de control. Ver Personalizar panel de control (en la página 263) para más información.

Azulejos cambian su estado y por lo tanto el color basado en los valores umbral establecidos en los umbrales del supervisor del sistema. Mientras que el sistema no establece algunos valores de umbral predeterminado para usted, usted puede decidir por sí mismo lo que el valor umbral debe ser para cada uno de los tres estados. Para configurar o cambiar valores de umbral, puede utilizar **Umbrales de monitor de sistema**. Ver Umbrales del monitor del sistema (explicado) (ver "Umbrales del monitor del sistema (explicados)" en la página 265).

Si una ficha cambia de color y desea saber qué servidor parámetro / que hace que el cambio de color del azulejo, haga clic en el azulejo. Esto abre una visión general en la parte inferior de la pantalla que muestra los colores rojo, amarillo o verde para cada parámetro de supervisión tiene habilitada para su azulejo. Haga clic en el botón **Detalles** para conseguir información detallada sobre los motivos del cambio de estado.

Si ve un signo de advertencia y coloca el mouse sobre él, el sistema le muestra un mensaje de error.

La funcionalidad del monitor del sistema requiere que el servicio Milestone XProtect Data Collector Server se esté ejecutando.

Personalizar panel de control

Añadir una nueva cámara o el azulejo del servidor

1. En la ventana de monitor de sistema, haga clic en **Personalizar**.
2. En la ventana **Personalizar panel del sistema** que se abre, haga clic en **Nueva** bajo **ventanas de servidor** o **ventanas cámara**.
3. En la nueva ventana **Nuevo azulejo servidor / baldosas cámara**, seleccionar las cámaras o servidores para vigilar.
4. Bajo **Control de parámetros,** active o desactive las casillas de verificación de los parámetros que se añaden o eliminan de la baldosa relevante.
5. Haga clic en **OK.** El nuevo servidor o baldosas de la cámara ahora se añade a las fichas que aparecen en el tablero de instrumentos.

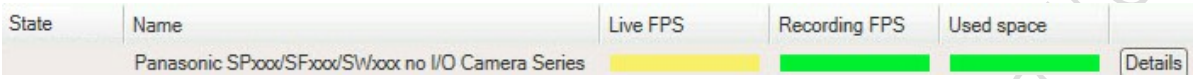
Editar parámetros de monitoreo

1. En la ventana de monitor de panel de control del sistema, haga clic en **Personalizar**.
2. En la ventana **Personalizar panel del sistema** que se abre, haga clic en **Editar** bajo **ventanas de servidor** o **ventanas de cámara**.
3. En ventana **Editar ficha servidor** o **Editar ficha cámara**, seleccione el componente de servidor o cámaras que desea editar.
4. En el **Control de parámetros** cuadro, active o desactive las casillas de verificación de los parámetros de supervisión que desea añadir o quitar de la baldosa relevante.
5. Haga clic en **OK**. Los parámetros de monitoreo cambiado son ahora una parte de o retirar material de la baldosa relevante.

Puede activar y desactivar los datos históricos en el sistema si así lo desea. Si deshabilita estos datos, no se puede ver gráficas de comportamiento del sistema anterior. Si desea reducir la carga en el servidor de base de datos SQL o en su ancho de banda, puede reducir el intervalo de muestreo de los datos históricos. Si se reduce el intervalo de muestreo de los datos históricos, menos detalles están disponibles en los gráficos.

Detalles del monitor del sistema (explicado)

Si hace clic en un azulejo del servidor o de la cámara, se puede ver el estado de cada parámetro de monitorización seleccionado debajo del tablero de instrumentos.



Ejemplo: REALES parámetros de supervisión de FPS de una cámara ha alcanzado el estado de advertencia.

El campo **Estado** muestra el estado de la cámara. Por ejemplo, una advertencia roja se muestra si la conexión con el dispositivo se rompe. El icono incluye una punta de la herramienta con una breve descripción del problema que está causando la advertencia.

Campo **Espacio utilizado** muestra datos de otros servidores de grabación donde este dispositivo tiene grabaciones si, por ejemplo, el dispositivo se ha situado en otros servidores de grabación previamente.

Si hace clic en el botón **Detalles** para la cámara/servidor relevante, puede ver la información del sistema y crear informes con respecto a:

Componente	Descripción
Servidor de gestión	Muestra los datos del servidor de gestión seleccionada
Servidor(es) de grabación	Muestra los datos del servidor de grabación seleccionado. Puede ver estos por: • Disco • Almacenamiento • Red • Cámara
Servidores de grabación Failover	Muestra los datos del servidor failover de grabación seleccionado.
Los servidores adicionales	Muestra los datos en el servidor de registro, servidores de eventos y más.
Cámaras	Muestra los datos de cualquier cámara en cualquier grupo de cámara en su configuración.

Cada uno de estos elementos es un área que usted puede hacer clic y expandirse. Al hacer clic en esta área, que ofrece datos dinámicos relevantes en este servidor o la cámara.

La barra **Cámaras** contiene una lista de grupos de cámaras para seleccionar. Una vez que se selecciona un grupo, seleccione una cámara específica y ver los datos dinámicos para ello. Todos los servidores muestran el

uso de la CPU y la información de la memoria disponible. Servidores de grabación también muestran información sobre el estado de conexión. Dentro de cada vista, encuentre un enlace **Historial**. Haga clic en él para ver datos históricos e informes (ver informes sobre una cámara, haga clic en el nombre de la cámara). Para cada informe histórico, se puede ver los datos de las últimas 24 horas, 7 días o 30 días. Para guardar y / o imprimir informes, haga clic en el icono **Enviar a PDF**. Utilice los iconos < y en casa para navegar Monitor de sistema.

Sólo se pueden crear informes históricos con los datos del servidor de grabación donde se encuentra actualmente el dispositivo.

Importante: Si tiene acceso a los detalles del monitor del sistema desde un sistema operativo de servidor, puede experimentar un mensaje con respecto a **Configuración de seguridad mejorada de Internet Explorer**. Siga las instrucciones en el mensaje para añadir página **Monitor de sistema** a la zona de **sitios de confianza** antes de continuar.

Umbrales del monitor del sistema (explicados)

Umbrales de monitor sistema le permiten configurar y ajustar los umbrales globales para cuando los azulejos en el monitor del sistema visual se debe indicar que el hardware del sistema cambia de estado, por ejemplo cuando el uso de la CPU de un servidor cambia desde un estado normal del estado (verde) a una advertencia estado (amarillo).

El sistema está configurado con los valores de umbral predeterminado para que pueda comenzar a supervisar el hardware del sistema desde el momento en que su sistema está configurado. Puede cambiar estos valores si desea (ver "Establecer umbrales de monitor del sistema" en la página 266).
Por defecto, el sistema está configurado para mostrar los valores de umbral para todas las unidades de un hardware en particular, por ejemplo, todas las cámaras o servidores. También puede configurar los valores de umbral para los servidores o cámaras individuales o un subconjunto de ellos. El establecimiento de valores de umbral para servidores o cámaras individuales puede ser una buena idea si, por ejemplo, algunas cámaras deben poder usar una mayor **FPS en directo** o **Grabando FPS** que otras cámaras.

Puede establecer los valores de umbral para servidores, cámaras, discos y almacenamiento. Si desea cambiar los valores de umbral, se puede utilizar el control deslizante de umbral. El control deslizante de umbral le permite aumentar o disminuir los valores de umbral arrastrando los controladores que separan los estados ya sea hacia arriba o hacia abajo. El control deslizante de umbral se divide en colores similares a los mostrados en las fichas de servidor o cámara presentes en el monitor sistema (ver "Monitor del sistema (explicado)" en la página 262).

Para asegurarse de que no se vea un estado **Crítica** o **Advertencia** en casos en los que el uso o la carga en el hardware del sistema alcanza un valor de umbral alto solo por un segundo o similar, utilice el **Intervalo de cálculo**. El **Intervalo de cálculo** promedia el efecto de cambios breves o frecuentes en un estado de hardware del sistema. En la práctica, esto significa que el **Intervalo de cálculo** nivela el efecto de los cambios de hardware en el tiempo de modo que usted no recibe alertas cada vez que se supera un umbral.

Por ejemplo, puede establecer el **Intervalo de cálculo** a un (1) minuto lo cual garantiza que sólo obtendrá alertas si el valor promedio de todo el minuto supera el umbral. La ventaja de esto es que evite las alertas sobre los cambios frecuentes y tal vez posiblemente irrelevantes en los estados de hardware y sólo recibir alertas que reflejan los problemas sostenidos con, por ejemplo, el uso de CPU o el consumo de memoria.

Umbrales de servidor

Límite	Descripción	Unidad
% uso de CPU	Los umbrales para el uso de la CPU en los servidores que supervisar.	%

Límite	Descripción	Unidad
Memoria disponible	Los umbrales para la memoria RAM en uso en los servidores que supervisar.	MB
Decodificación de NVIDIA	Umbrales para el uso de decodificación de NVIDIA en los servidores que supervisa.	%
Memoria de NVIDIA	Umbrales para la memoria RAM NVIDIA en uso en los servidores que supervisa.	%
Procesamiento de NVIDIA	Umbrales para el uso de representación de NVIDIA en los servidores que supervisa.	%

Los umbrales de la cámara

Límite	Descripción	Unidad
FPS en directo	Los umbrales para las cámaras FPS 'en uso cuando el vídeo en directo se muestra en las cámaras se realiza un seguimiento.	%
Grabando FPS	Los umbrales para las cámaras FPS 'en su uso cuando el sistema está grabando el vídeo de las cámaras se realiza un seguimiento.	%
Espacio utilizado	Los umbrales para el espacio utilizado por las cámaras se realiza un seguimiento.	GB

Umbrales de disco

Límite	Descripción	Unidad
Espacio libre	Los umbrales para el espacio disponible en los discos se realiza un seguimiento.	GB

Umbrales de almacenamiento

Límite	Descripción	Unidad
Periodo de retención	Umbral que muestra una predicción para cuando se queda sin espacio en su almacenamiento. El estado que se muestra se basa en la configuración de su sistema y se actualiza dos veces al día.	Días

También puede configurar reglas (ver "Reglas (explicadas)" en la página 203) para realizar acciones específicas o activar alarmas (ver "Alarmas (explicado)" en la página 274) cuando un umbral de cambios de un estado a otro.

Establecer umbrales de monitor del sistema

1. Seleccione la casilla de verificación **Habilitar** para el hardware del sistema relevante si aún no lo ha permitido

2. Arrastre el control deslizante de umbral arriba o hacia abajo para aumentar o disminuir el valor de umbral. Hay dos controles deslizantes disponibles para cada pieza de hardware del sistema se muestra en el control de umbral, que separan los niveles **Normal**, **Advertencia** y **Críticos**.

3. Una vez que haya establecido los niveles umbrales correspondientes, seleccione **Archivo** > **Guardar** del menú.

Un ejemplo de cómo se puede establecer un deslizador de control de umbral. Arrastre los controles deslizantes hacia arriba y hacia abajo para aumentar o disminuir cualquiera de los tres niveles de umbral. El color rojo indica que ha llegado a un estado crítico, amarillo es un estado de advertencia que indica que está a punto de alcanzar el estado crítico y verde indica que las cosas están en un estado normal y dentro de sus valores umbrales seleccionados.

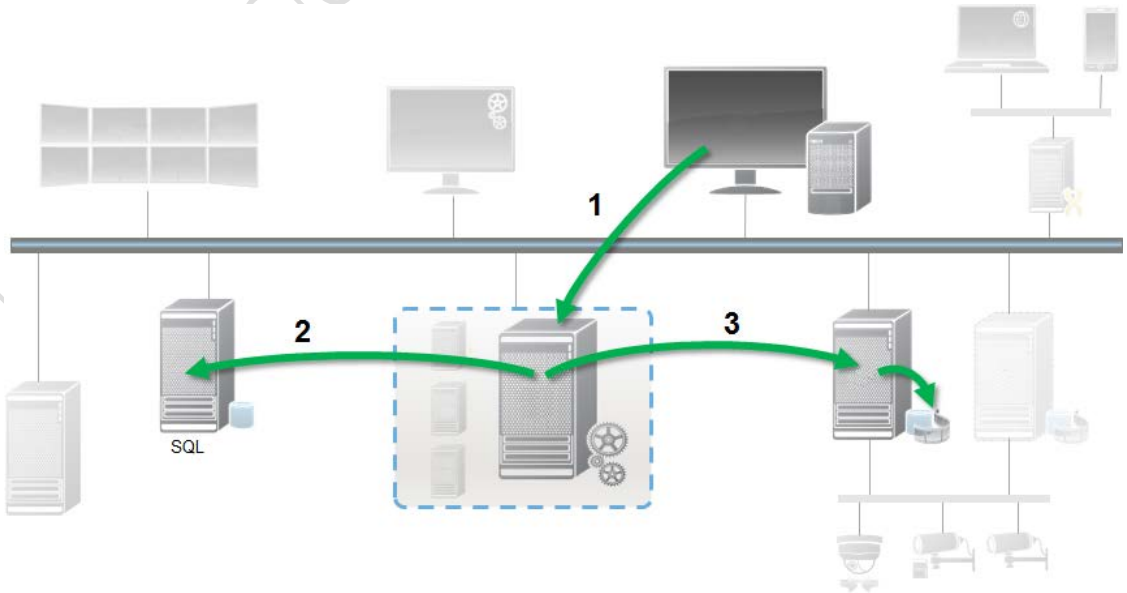
Bloqueo de evidencia (explicado)

Funcionalidad disponible depende del sistema que está utilizando. Ver tabla de comparación de productos (en la página 24) para más información.

Con la funcionalidad de bloqueo de evidencias, los operadores de los clientes pueden proteger a las secuencias de vídeo, incluyendo audio y otros datos, desde su eliminación, si es necesario, por ejemplo, mientras una investigación o juicio está en curso. Para obtener información sobre cómo bloquear pruebas, consulte la documentación de XProtect Smart Client.

Cuando está protegido, los datos no se pueden borrar, ni automáticamente por el sistema después de un tiempo de retención predeterminado del sistema o en otras situaciones, ni manualmente por los usuarios del cliente. El sistema o un usuario no puede borrar los datos hasta que un usuario con derechos de usuario suficientes desbloquea la evidencia.

Diagrama de flujo para el Bloqueo de evidencias:



1. El usuario crea un Bloqueo de evidencias en XProtect Smart Client. La información enviada al servidor de gestión.
2. Management Server almacena información sobre el bloqueo de evidencias en el servidor SQL.
3. Management Server informa de grabación del servidor para almacenar y proteger las grabaciones protegidas en la base de datos.

Cuando el operador crea un bloqueo de evidencias, los datos protegidos permanecen en el almacenamiento de grabación que se graba en, y se mueve a los discos de archivado junto con los datos no protegidos, pero los datos protegidos:

- Sigue el tiempo de retención configurado para el bloqueo de evidencias. Potencialmente infinitamente.
- Mantiene la calidad original de las grabaciones, incluso si el aseo se ha configurado para datos no protegidos.

Cuando un operador crea bloqueos, el tamaño mínimo de una secuencia es el período en el que la base de datos se divide en archivos grabados, esto es, con secuencias predeterminadas de una hora. Puede cambiar esto, pero requiere que personaliza el archivo RecorderConfig. xml en el servidor de grabación. Si una pequeña secuencia abarca dos períodos de una hora, el sistema bloquea las grabaciones en ambos períodos.

En el registro de auditoría del Management Client, se puede ver cuando un usuario crea, edita o elimina bloqueo de evidencias.

Cuando un disco se queda sin espacio en disco, no tiene impacto en los datos protegidos. En su lugar se eliminarán los datos no protegidos más antiguos. Si no hay más datos no protegidos que eliminar, el sistema deja de grabar. Puede crear reglas y alarmas activadas por eventos de disco completo, por lo que se le notifica automáticamente.

Excepto para más datos que se almacena durante un período más largo y afectando potencialmente almacenamiento en disco, la función de bloqueo de evidencias, como tal, no influye en el rendimiento del sistema.

Si movimiento de hardware (ver "Hardware móvil (explicado)" en la página 112) a otro servidor de grabación:

- Grabaciones protegidas con bloqueo de evidencias, permanece en el servidor de grabación de edad tras el tiempo de retención establecido para el bloqueo de evidencias, cuando fue creado.
- El usuario XProtect Smart Client todavía puede proteger los datos con bloqueos de evidencia de las grabaciones que se hicieron en una cámara que se movió a otro servidor de grabación. Incluso si se mueve la cámara varias veces y las grabaciones se almacenan en múltiples servidores de grabación.

Por defecto, todos los operadores tienen el perfil de bloqueo de evidencia por defecto asignado a ellos, pero no los derechos de acceso del usuario a la función. Para especificar los derechos de acceso de bloqueo de la evidencia de un cometido, consulte la ficha Dispositivo (ver "Pestaña Dispositivo (cometidos)" en la página 251) para la configuración de los cometidos.Para especificar el perfil de bloqueo de evidencia de un cometido, consulte la ficha Info (ver "Pestaña Información (cometidos)" en la página 232) para la configuración de los cometidos.

En el Management Client, puede editar las propiedades del perfil de bloqueo de evidencia por defecto y crear perfiles de bloqueo de evidencia adicionales y asignar éstos a los cometidos en su lugar.

Bloqueo de evidencia bajo **Panel del sistema** muestra una visión general de todos los datos protegidos en el sistema de vigilancia actual:

- fecha de inicio y final de los datos protegidos
- el usuario que bloqueó la evidencia
- cuando la evidencia ya no está bloqueada

- donde se almacenan los datos
- el tamaño de cada bloqueo de evidencia

Toda la información que se muestra en **Bloqueo de evidencias** son instantáneas. Presione F5 para actualizar.

Tareas actuales (explicadas)

El nodo **Tareas actuales** muestra una vista general de las tareas en un servidor de grabación seleccionado, su hora de inicio, la hora de finalización estimada y el progreso. Toda la información que se muestra en **Las tareas actuales** son instantáneas. Puede actualizar estos haciendo clic en el botón de **Actualizar** en la esquina inferior derecha de las **propiedades** panel.

Informes de configuración (explicados)

Al crear informes de configuración de PDF, puede incluir todos los elementos posibles de su sistema en el informe. Puede, por ejemplo, incluir licencias, configuración de dispositivos, configuración de alarmas, y mucho más. También puede personalizar la configuración de fuentes y páginas e incluir una portada personalizada.

Añadir un informe de configuración

1. Expanda **Panel del sistema** y haga clic en **Informes de configuración**. Esto nos lleva a la página de configuración del informe.
2. Seleccione los elementos que desea incluir en el informe.
3. **Opcional**: Haga clic en **Página frontal** para personalizar su portada. En la ventana que aparece, rellene la información necesaria. Seleccionar **Página inicial** como un elemento que incluya en que informe, de lo contrario la primera página se personaliza no está incluido en el informe.
4. Haga clic en **Formateando** para personalizar su fuente, tamaño de página y márgenes. En la ventana que aparece, seleccione los ajustes deseados.
5. Cuando esté listo para exportar, haga clic en **Exportar** y seleccione un nombre y una ubicación para guardar para que informe.

Configurar los detalles del informe

El siguiente está disponible cuando la creación de informes:

Nombre	Descripción
Selec. todo	Selecciona todos los elementos de la lista.
Limpiar todo	Borra todos los elementos de la lista.
Página delantera	Personalizar la primera página del informe.
Formateo	Formatear el informe.
Exportación	Seleccione una ubicación para guardar el informe y crear un archivo PDF.

Registros de servidores

Registros (explicados)

Puede ver y exportar contenidos de diferentes registros relacionados con el sistema. El propósito de los registros es documentar actividad, eventos, acciones y errores en el sistema, para el análisis o la documentación más tarde.

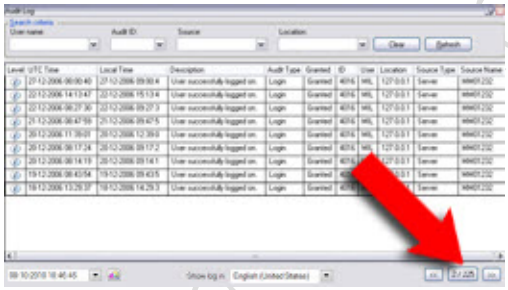
Los registros tienen diferentes propósitos:

Nombre	Descripción
Registro del sistema	Relativos al sistema de registros de información.
Registro de auditorías	Registros de la actividad del usuario.
Registro de reglas	Normas registros en los que los usuarios se hayan especificado en la nueva acción Hacer entrada de registro.

El sistema tiene un número de ajustes predeterminados relacionados con los diferentes registros. Para cambiar la configuración, consulte los registros del servidor (ver "Los registros del servidor de la ficha (opciones)" en la página 284) pestaña de Opciones.

Puede ver los registros en un número de diferentes idiomas (ver "Cambiar el idioma de registro" en la página 271) y los registros de exportación (ver "Trozas de exportación" en la página 271) como archivos delimitado por tabuladores de texto (.txt).

Si un registro contiene más de una página de información, puede navegar entre las páginas de registro haciendo clic en los botones en la esquina inferior derecha del panel de registro:



En la esquina inferior izquierda, saltar a una fecha y hora específica en el registro:

Buscar en los registros

Para buscar un registro, utilice **criterios de búsqueda** en la parte superior del panel de registro:

1. Especifique los criterios de búsqueda en las listas.
2. Haga clic en **Actualizar** para que la página de registro refleje sus criterios de búsqueda. Para borrar los criterios de búsqueda y volver a la visualización de todos los contenidos de registro, haga clic en **Borrar**.

Puede hacer doble clic en cualquier fila para tener todos los detalles presentados en una ventana **Detalles del registro**. De esta manera también se puede leer las entradas del registro que contienen más texto del que se puede mostrar en una sola línea.

Trozas de exportación

Puede exportar los registros como archivos delimitado por tabuladores de texto (. txt). Puede personalizar el contenido del registro especificando qué registro, elementos de registro, y de tiempo para incluir en la exportación. Por ejemplo, puede especificar que sólo incluya las entradas de registro relacionadas con el error del registro del sistema entre el 2 de enero de 2016 a las 08:00:00 y el 6 de enero de 2014 a las 07:59:59 en su exportación.

Para exportar un registro:

1. En campo **Nombre de archivo** de la ventana **Registro de exportación**, especifique un nombre para el archivo de registro exportado.

   De forma predeterminada, los archivos de registro exportados se guardan en la carpeta **Mis documentos**. Sin embargo, puede especificar una ubicación diferente haciendo clic en el botón Examinar junto al campo.

2. Los criterios que ha seleccionado para orientar el contenido del registro exportado se enumeran en el campo **Filtros**. No puede editar este campo. Si necesita cambiar su criterio, cerrar la ventana, y repita los pasos 1-2.

3. Especificar el período de tiempo que desea que la exportación a cubrir. Especifique **Fecha y hora de inicio** y **Fecha y hora de finalización de los campos** respectivamente. Se puede seleccionar la fecha haciendo clic en la flecha:

   Para especificar una hora exacta, sobrescribir los elementos necesarios de tiempo (horas: minutos: segundos) con los valores necesarios. En este ejemplo, el elemento horas se sobrescribe:

4. Haga clic **Exportar** para exportar el contenido del registro.

Cambiar el idioma de registro

1. En la parte inferior del panel de registro, en lista **Mostrar inicio de sesión**, seleccionar el idioma deseado.

2. El registro se mostrará en el idioma seleccionado. La próxima vez que su abierto el registro, se vuelve a situar el idioma por defecto.

Registro del sistema (propiedades)

Cada fila representa un registro de una entrada de registro. Una entrada de registro contiene una serie de campos de información:

Nombre	Descripción
Nivel	Muestra un icono que indica el nivel de la entrada de registro: - indica información - indica una advertencia - indica un error "En blanco" - indica una entrada sin definir.
Hora UTC	Fechados en el tiempo universal coordinado (UTC).
Hora local	Fechados en la hora local del servidor de su sistema.
ID	El número de identificación para el incidente registrado.
Tipo de fuente	El tipo de equipo en el que se produjo el incidente registrado, por ejemplo, un servidor o dispositivo.
Nombre de fuente	Servidor de gestión, el nombre del servidor de grabación o dispositivo en el que se produjo el incidente registrado.
Tipo de evento	El tipo de evento representado por el incidente registrado.
Descripción	Muestra una descripción del incidente registrado.

Registro de auditoría (propiedades)

Cada fila representa un registro de una entrada de registro. Una entrada de registro contiene una serie de campos de información:

Nombre	Descripción
Nivel	Muestra un icono que indica el nivel de la entrada de registro: - indica información - indica una advertencia - indica un error "En blanco" - indica una entrada sin definir.
Hora UTC	Fechados en el tiempo universal coordinado (UTC).
Hora local	Fechados en la hora local del servidor de su sistema.
ID	El número de identificación para el incidente registrado.
Usuario	El nombre de usuario del usuario remoto causando el incidente registrado.
Ubicación de usuario	La dirección IP o nombre de host del equipo desde el que el usuario remoto causó el incidente registrado.
Permiso	La información acerca de si se permitió que la acción del usuario remoto (concedido) o no.
Categoría	El tipo de incidente registrado.
Tipo de recurso	El tipo de equipo en el que se produjo el incidente registrado, por ejemplo, un servidor o dispositivo.

Nombre	Descripción
Nombre de recurso	Servidor de gestión, o el nombre del servidor de grabación o dispositivo en el que se produjo el incidente registrado.
Host de recursos	El nombre del servidor que aloja la grabación de un dispositivo o un almacenamiento en el que se produjo el incidente registrado. El nombre del servidor de gestión que aloja el servidor de grabación o el servidor de gestión en que se produjo el incidente registrado.
Descripción	Muestra una descripción del incidente registrado.

Regla log (propiedades)

Cada fila representa un registro de una entrada de registro. Una entrada de registro contiene una serie de campos de información:

Nombre	Descripción
Nivel	Muestra un icono que indica el nivel de la entrada de registro: - indica información - indica una advertencia - indica un error "En blanco" - indica una entrada sin definir.
Hora UTC	Fechados en el tiempo universal coordinado (UTC).
Hora local	Fechados en la hora local del servidor de su sistema.
ID	El número de identificación para el incidente registrado.
Nombre de servicio	El nombre del servicio en el que se produjo el incidente registrado.
Nombre de regla	El nombre de la regla de la activación de la entrada de registro.
Tipo de fuente	El tipo de equipo en el que se produjo el incidente registrado, por ejemplo, un servidor o dispositivo.
Nombre de fuente	Servidor de gestión, el nombre del servidor de grabación o dispositivo en el que se produjo el incidente registrado.
Tipo de evento	El tipo de evento representado por el incidente registrado.
Tipo de generador	El equipo pf tipo en el que se desencadenó el incidente registrado. Las entradas de registro son definidas por el administrador y se refieren a incidentes en el sistema.
Nombre de generador	El nombre del equipo en el que se generó el incidente registrado.
Descripción	Muestra una descripción del incidente registrado.

Alarmas

Alarmas (explicado)

Importante: Esta función sólo funciona si tiene instalado el servidor de eventos XProtect.

Sobre la base de la funcionalidad manejado en el servidor de eventos, cuentan con las alarmas presenta un panorama central, el control y la escalabilidad de las alarmas en cualquier número de instalaciones (incluyendo cualesquiera otros sistemas XProtect) en toda la organización. Se puede configurar para generar alarmas de la base de:

- **Eventos relacionados con el sistema interno**

  Por ejemplo, el movimiento, respondiendo servidor / no responde, el archivo de problemas, la falta de espacio en disco y más.

- **Eventos externos integrados**

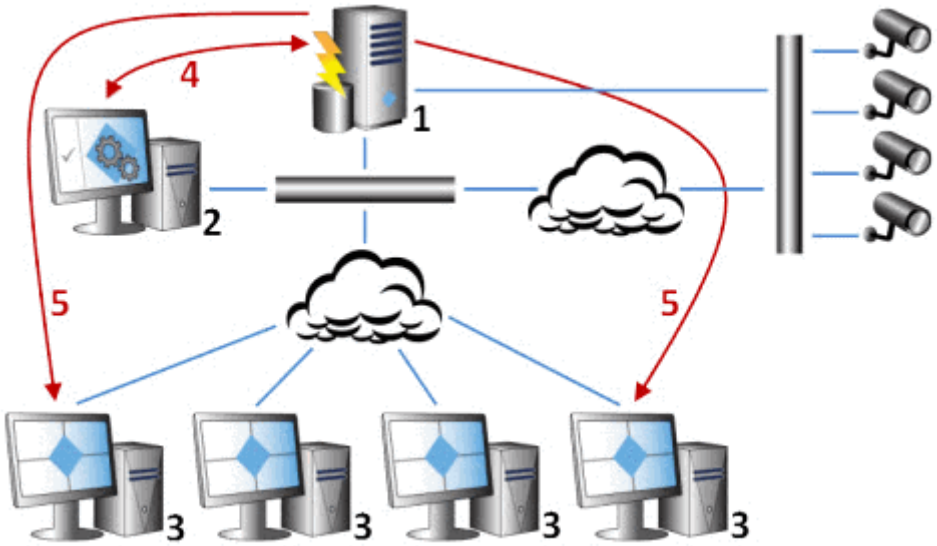
  Este grupo puede consistir en varios tipos de eventos externos:

  - **Eventos analíticos**

    Normalmente, los datos recibidos de un análisis de contenido de vídeo de terceros externa (VCA) proveedores.

  - **MIP eventos de plug-in**

    A través del kit de desarrollo de software (SDK) MIP, un proveedor externo puede desarrollar complementos personalizados (por ejemplo, integración con sistemas de control de acceso externos o similares) a su sistema.



Leyenda:

1. Sistema de vigilancia
2. Management Client
3. XProtect Smart Client
4. Configuración de alarmas
5. El flujo de datos de alarma

Manejar y delegar las alarmas en la lista de alarmas en XProtect Smart Client. También puede integrar la funcionalidad de alarmas con el mapa del XProtect Smart Client.

Configuración de alarma (explicada)

Configuración de alarmas incluye:

- Configuración basada en cometido dinámico de gestión de alarmas
- Descripción técnica general sobre el centro de todos los componentes: servidores, cámaras y unidades externas
- Configuración de la central de registro de todas las alarmas entrantes y la información del sistema
- Manipulación de plug-ins, lo que permite una integración personalizada de otros sistemas, por ejemplo, el control de acceso externo o sistemas basados en VCA.

En general, las alarmas son controladas por la visibilidad del objeto que causa la alarma. Esto significa que los cuatro aspectos posibles pueden desempeñar un cometido en lo que respecta a las alarmas y que pueden controlar / gestionar ellos y en qué medida:

Nombre	Descripción
Fuente visibilidad / dispositivo	Si el dispositivo que causa la alarma no está configurado para ser visible al cometido del usuario, el usuario no puede ver la alarma en la lista de alarmas en XProtect Smart Client.
El derecho a desencadenar eventos definidos por el usuario	Este derecho determina si el cometido del usuario puede desencadenar eventos definidos por el usuario seleccionado en XProtect Smart Client.
Plug-ins externos	Si ningún plug-ins externos se configuran en el sistema, estos podrían controlar los derechos de los usuarios para manejar las alarmas.
Derechos general de cometido	Determine si el usuario sólo puede ver o gestionar alarmas. Lo que un usuario de **alarmas** puede hacer con alarmas depende del cometido del usuario y de la configuración configurados para ese cometido particular.

En **Alarms and Events** ficha en **Opciones** , puede especificar la configuración de alarmas, eventos y registros.

Definiciones de alarma

Cuando el sistema registra un suceso en el sistema, se puede configurar el sistema para generar una alarma en XProtect Smart Client. Debe definir las alarmas antes de poder utilizarlos, y las alarmas se definen basándose en los acontecimientos registrados en los servidores del sistema. También puede utilizar los eventos definidos por el usuario para activar las alarmas y utilizar el mismo evento para activar varias alarmas diferentes.

Añadir una alarma

Para definir una alarma, es necesario crear una definición de alarma, donde se especifica, por ejemplo, lo que dispara la alarma, instrucciones sobre lo que el operador tiene que hacer, y qué o cuando se apague la alarma. Para obtener información detallada sobre los ajustes, consulte Definiciones de alarma (propiedades) (en la página 277).

1. En el panel **Navegación del sitio**, expanda **Alarmas** y haga clic con el botón secundario en **Definiciones de alarma**.
2. Selecciona **Añadir Nuevo**.
3. Rellene estas propiedades:
   - **Nombre**: Escriba un nombre para la definición de alarma. El nombre de la definición de alarma aparece cada vez que aparece la definición de alarma.
   - **Instrucciones**: Se puede escribir instrucciones para el operador que recibe la alarma.

- **Evento de activación**: Utilice los menús desplegables para seleccionar un tipo de evento y un mensaje de evento que se utilizarán cuando se active la alarma.

  Una lista de eventos de activación seleccionables. El que puso de relieve que se crea y personalizar mediante eventos analíticos.

- **Fuentes**: Seleccione las cámaras u otros dispositivos que el evento debe proceder de activar la alarma. Sus opciones dependen del tipo de evento que ha seleccionado.

- **Perfil temporal**: Si desea que la alarma se active durante un intervalo de tiempo específico, seleccione el botón de opción y, a continuación un perfil temporal en el menú desplegable.

- **Evento basado en:** Si desea que la alarma se activa mediante un evento, seleccione el botón de opción y especificar qué evento se iniciará la alarma. También es necesario especificar el evento que va a parar la alarma.

4. En el límite **menú desplegable** Tiempo, especificar un límite de tiempo para cuando se requiere una acción por parte del operador.

5. En menú desplegable **Eventos activados**, especifique qué evento para activar cuando se ha superado el límite de tiempo.

6. Especificar los ajustes adicionales, por ejemplo, relacionados con las cámaras y propietario inicial de alarma.

Definiciones de alarma (propiedades)

La tabla se describen los ajustes que puede realizar cuando se crea una definición de alarma.

Configuración de la definición de alarma:

Nombre	Descripción
Habilitar	Por defecto, la definición de alarma está activada. Para desactivarla, desactive la casilla de verificación.
Nombre	Nombres de alarma no tienen que ser único, pero utilizando nombres exclusivos y descriptivos de alarma son ventajosos en muchas situaciones.
Instrucciones	Escriba un texto descriptivo sobre la alarma y la forma de resolver el problema que causó la alarma. El texto aparece en XProtect Smart Client cuando el usuario se encarga de la alarma.

Nombre	Descripción
Evento desencadenante	Seleccione el mensaje de evento para utilizar cuando se dispara la alarma. Elegir entre dos menús desplegables: • El primer menú desplegable: Seleccione el tipo de evento, por ejemplo, evento de analytics y eventos del sistema. • El segundo desplegable: Seleccione el mensaje de evento específico para utilizarlo. Los mensajes disponibles están determinados por el tipo de evento que ha seleccionado en el primer menú desplegable.
Fuentes	Especificar las fuentes que se originan a partir de los acontecimientos. Aparte de las cámaras u otros dispositivos, las fuentes también pueden ser plug-in de fuentes definidas, por ejemplo VCA y MIP. Las opciones dependen del tipo de evento que haya seleccionado.

Disparador de la alarma:

Nombre	Descripción
Perfil temporal	Seleccione el botón de selección **Perfil temporal** para especificar el intervalo de tiempo durante el cual está activa la definición de alarma. Sólo el perfil temporal que ha definido en el nodo **Reglas y eventos** se muestra en la lista. Si no se definen, sólo está disponible la opción **Siempre**.
Basado en eventos	Si desea que la alarma debe basarse en un evento, seleccione este botón de radio. Una vez seleccionado, especifique el inicio y parada evento. Puede seleccionar eventos de hardware definidos en las cámaras, los servidores de vídeo y la entrada (ver "Visión general Eventos" en la página 194). También se pueden utilizar definiciones de eventos globales / manuales (ver "Eventos definidos por el usuario (explicados)" en la página 218).

Acción requiere de un operador:

Nombre	Descripción
Límite de tiempo	Seleccionar un límite de tiempo para cuando se requiere acción del operador. El valor por defecto es de 1 minuto. El límite de tiempo no se activa antes de que haya conectado un evento en los **eventos activados** menú desplegable.
Eventos activados	Seleccionar las citas que se disparan cuando ha pasado el límite de tiempo.

Ajustes adicionales:

Nombre	Descripción
Cámaras relacionados	Seleccione un máximo de 15 cámaras a incluir en la definición de alarma, incluso si estas cámaras mismas no activan la alarma. Esto puede ser relevante, por ejemplo, si ha seleccionado un mensaje de evento externo (por ejemplo, se abre una puerta) como la fuente de la alarma. Mediante la definición de una o más cámaras cerca de la puerta, puede adjuntar grabaciones del incidente de la cámara a la alarma.
Mapa Relacionados	Asignar un mapa para la alarma cuando aparece en el **Gestor de alarma** del XProtect Smart Client .
Propietario alarma inicial	Seleccionar un usuario por defecto responsable de la alarma.
Prioridad de la alarma inicial	Seleccione una prioridad (**Alta**, **Medio**, **Baja** o ninguna) para la alarma. Utilice estas prioridades en XProtect Smart Client para determinar la importancia de una alarma.
categoría de alarma inicial	Seleccione una categoría de alarma para la alarma, por ejemplo **Falsa alarma** o **Es necesario investigar**.
Eventos activados por la alarma	Definir un evento que puede desencadenar la alarma en el XProtect Smart Client.
Alarma de auto-cierre	Si quieres un evento en particular para detener automáticamente la alarma, seleccione esta casilla de verificación. No todos los eventos pueden activar alarmas. Desactive la casilla de verificación para desactivar la alarma de nuevo desde el principio.

Ver también

Añadir una alarma (en la página 276)

Ajustes de alarma de Datos

Al configurar los ajustes de datos de alarma, especifique lo siguiente:

Alarma de datos ficha Niveles

Prioridades

Nombre	Descripción
Nivel	Añadir nuevas prioridades con números de nivel de su elección o el uso / editar los niveles de prioridad por defecto (números 1, 2 o 3). Estos niveles de prioridad se utilizan para configurar el ajuste de la **alarma inicial prioridad**.
Nombre	Escriba un nombre para la entidad. Puede crear tantos como te gusta.
Sonar	Seleccione el sonido que se asocia con la alarma. Utilice uno si los sonidos predeterminados o añadir más de los **parámetros de sonido**.

Estados

Nombre	Descripción
Nivel	Además de los niveles de estado predeterminados (números **1**, **4**, **9** y **11**, que no se pueden editar ni reutilizar), añadir nuevos estados con números de nivel de su elección. Estos niveles de estado sólo son visibles en la lista alarma del XProtect Smart Client .

Categorías

Nombre	Descripción
Nivel	Añadir nuevas categorías con números de nivel de su elección. Estos niveles de categoría se utilizan para configurar categoría ajuste de la **alarma inicial**.
Nombre	Escriba un nombre para la entidad. Puede crear tantos como te gusta.

Pestaña de Configuración de lista alarma

Nombre	Descripción
Columnas disponibles	Utilice> para seleccionar qué columnas deben estar disponibles en la lista de alarmas de XProtect Smart Client. Utilice <clara a la selección. Cuando haya terminado, **columnas seleccionadas** deben contener los elementos que deben incluirse.

Razones para la pestaña de cierre

Nombre	Descripción
Habilitar	Seleccionar para permitir que todas las alarmas se deben asignar una razón para el cierre antes de que puedan ser cerradas.
Razón	Añadir razones para el cierre que el usuario puede elegir entre el momento de cerrar las alarmas. Los ejemplos podrían ser Resuelto-Intruso o Falsa Alarma. Puede crear tantos como te gusta.

Ajustes de sonido

Al configurar los ajustes de sonido, especifique lo siguiente:

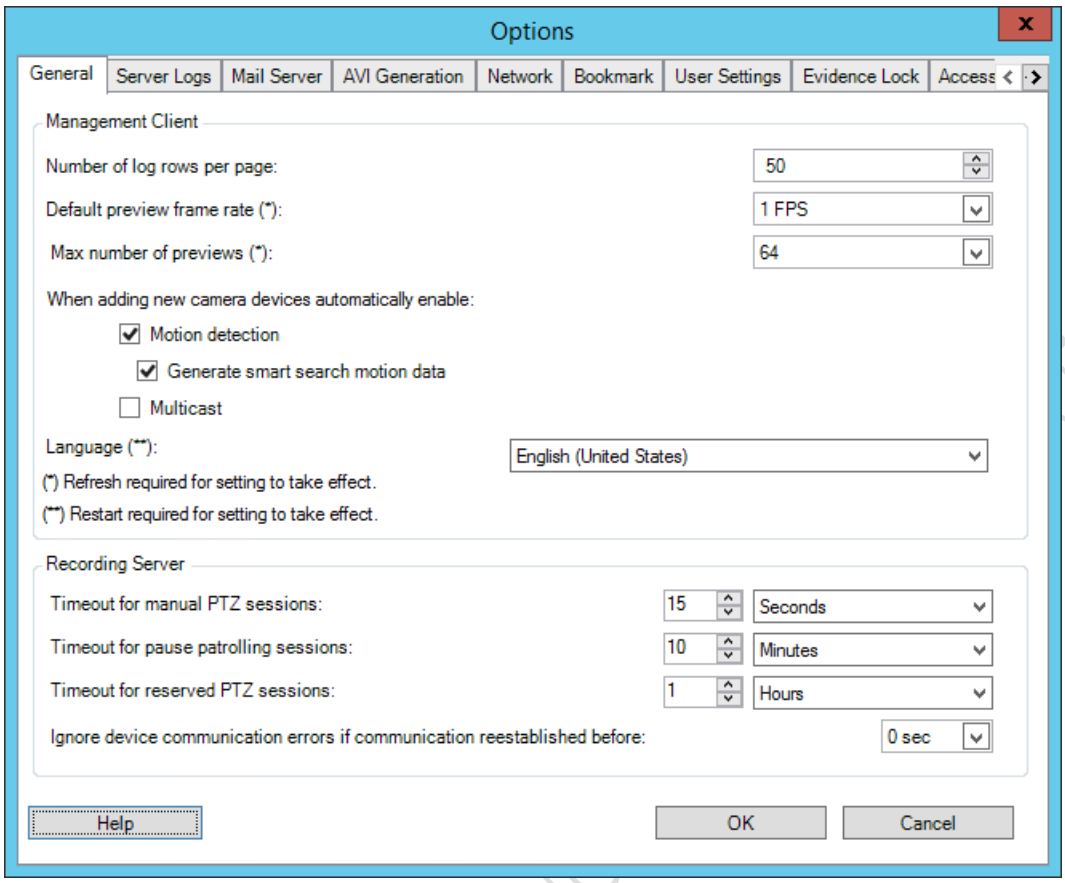
Nombre	Descripción
Sonidos	Seleccione el sonido en asociar a la alarma. La lista de sonidos contiene varios sonidos predeterminados de Windows. No puede editar estos. Sin embargo, puede añadir nuevos sonidos del tipo de archivo . wav, pero sólo si éstos están codificados en modulación por impulsos codificados (PCM). Incluso si los sonidos predeterminados son sonoros archivos estándar de Windows, la configuración de Windows locales podrían hacer que estos sonidos diferentes en máquinas diferentes. Algunos usuarios también podrían haber eliminado uno o más de estos archivos sonoros y por lo tanto no pueden jugar con ellos. Para garantizar un sonido idéntico en todo, debe importar y utilizar sus propios archivos . wav codificados en PCM.
Añadir	Añadir sonidos. Explorar con el sonido de cargar uno o varios archivos . wav.
Borrar	Retirar un sonido seleccionado de la lista de sonidos añadidos manualmente. Sonidos predeterminados no se pueden eliminar.
Probar	Probar el sonido. En la lista, seleccione el sonido. El sonido se reproduce una vez.

Cuadro de diálogo opciones

En el cuadro de diálogo **Opciones**, puede especificar un número de configuraciones relacionadas con el aspecto general y la funcionalidad del sistema.

Funcionalidad disponible depende del sistema que está utilizando. Ver tabla de comparación de productos (en la página 24) para más información.

Para acceder al cuadro de diálogo, seleccione **Herramientas** > **Opciones**.



El cuadro de diálogo **Opciones** dispone de las siguientes fichas:

- Pestaña General (ver "Pestaña General (opciones)" en la página 283)
- Pestaña Registros de servidor (ver "Los registros del servidor de la ficha (opciones)" en la página 284)
- Pestaña Servidor de correo (ver "Pestaña Servidor de correo (opciones)" en la página 285)
- Pestaña Generación AVI (ver "Pestaña Generación AVI (opciones)" en la página 286)
- Pestaña red (ver "Pestaña Red (opciones)" en la página 287)
- Pestaña marcador (ver "Pestaña Favoritos (opciones)" en la página 287)
- Pestaña Configuración de usuario (ver "Pestaña configuración de usuario (opciones)" en la página 287)
- Pestaña de bloqueo de evidencia (ver "Pestaña Bloqueo de evidencias (opciones)" en la página 287)
- Pestaña de mensajes de audio (ver "Pestaña de mensajes de audio (opciones)" en la página 288)
- Pestaña Configuración de Control de Acceso (ver "Pestaña Configuración de control de acceso (opciones)" en la página 289)
- Pestaña Analytics Eventos (ver "Pestaña eventos analíticos (opciones)" en la página 289)
- Ficha Alarmes y eventos (ver "Ficha Alarmas y eventos (opciones)" en la página 290)
- Pestaña Eventos genéricos (ver "Pestaña eventos genéricas (opciones)" en la página 291)

Pestaña General (opciones)

En la ficha General, puede especificar la configuración general del Management Client y el servidor de grabación.

Management Client

Nombre	Descripción
Número de filas por página de registro	Seleccione el número de filas de una sola página de registro puede contener. El valor por defecto es de 50 filas. Si un registro contiene más filas, que muestra las siguientes filas en las páginas siguientes.
Frecuencia de imagen de vista previa por defecto	Seleccione la velocidad de fotogramas para las imágenes de la cámara en miniatura que se muestran en el panel **Prever**. El valor predeterminado es 1 fotograma por segundo. Seleccione **Acción** > **Actualizar** desde el menú para que el cambio surta efecto. Tenga en cuenta que una velocidad de fotogramas alta en combinación con un gran número de imágenes en miniatura en el panel **Prever** ralentiza el equipo que ejecuta el Management Client. Puede limitar el número de imágenes en miniatura con ajuste **Número máximo de previsualizaciones**.
Número máximo de vistas previas	Seleccione el número máximo de imágenes en miniatura que se muestran en el panel **Prever**. Por defecto es de 64 imágenes en miniatura. Seleccione **Acción** > **Actualizar** desde el menú para que el cambio surta efecto. Tenga en cuenta que un gran número de imágenes en miniatura en combinación con una alta velocidad de cuadro puede ralentizar el sistema. Puede limitar la velocidad de fotogramas utilizado para las imágenes en miniatura con la configuración por **Velocidad de fotogramas de previsualización predeterminada**.
Al añadir nuevos dispositivos de cámara activar automáticamente: **Detección de movimiento**	Seleccione la casilla de verificación para activar la detección de movimiento en las nuevas cámaras cuando las añadir al sistema con el asistente **Añadir hardware**. Este ajuste no afecta a la configuración de detección de movimiento en las cámaras existentes. Permite activar y desactivar la detección de movimiento para una cámara en la pestaña **Movimiento** de la cámara del dispositivo.
Al añadir nuevos dispositivos de cámara activar automáticamente: **Generar datos de movimiento para búsqueda avanzada**	Generación de datos de movimiento para la búsqueda avanzada requiere que la detección de movimiento está habilitada para la cámara. Active la casilla de verificación para activar la generación de datos de movimiento de búsqueda inteligente en nuevas cámaras, al añadirlas al sistema con el asistente **Añadir hardware**. Este ajuste no afecta a la configuración de detección de movimiento en las cámaras existentes. Permite activar y desactivar la generación de datos de búsqueda avanzada de movimiento de una cámara en la pestaña **Movimiento** de la cámara del dispositivo.

Nombre	Descripción
Al añadir nuevos dispositivos de cámara activar automáticamente: **Multidifusión**	Seleccione la casilla de verificación para activar la multidifusión en nuevas cámaras cuando se agregan con el Asistente **Añadir hardware**. Este ajuste no afecta a la configuración de multidifusión en las cámaras existentes. Permite activar y desactivar la multidifusión en vivo para una cámara en la pestaña **Cliente** para la cámara del dispositivo.
Idioma	Seleccionar el idioma del Management Client. Reiniciar el Management Client para utilizar el nuevo idioma.

Servidor de grabación

Nombre	Descripción
Tiempo de espera para las sesiones de PTZ manuales	Los usuarios de clientes con los derechos de usuario necesarios pueden interrumpir manualmente el patrullaje de las cámaras PTZ. Seleccione cuánto tiempo debe pasar antes de patrullaje regular se reanudó después de una interrupción manual. El ajuste se aplica a todas las cámaras PTZ en su sistema. El ajuste por defecto es de 15 segundos. Si desea tiempos de espera en las cámaras individuales, se especifica esto en la pestaña **Posiciones predefinidas** para la cámara.
Tiempo de espera para las sesiones de pausa de patrullaje	Los usuarios de clientes con una prioridad suficiente PTZ pueden hacer una pausa en el patrullaje de las cámaras PTZ. Seleccione cuánto tiempo debe pasar antes de patrullaje regular se reanudó después de una pausa. El ajuste se aplica a todas las cámaras PTZ en su sistema. El ajuste por defecto es de 10 minutos. Si desea tiempos de espera en las cámaras individuales, se especifica esto en la pestaña **Posiciones predefinidas** para la cámara.
Tiempo de espera para las sesiones de PTZ reservados	Establecer el período de tiempo de espera predeterminado para las sesiones de PTZ reservados. Cuando un usuario ejecuta una sesión reservada PTZ, la cámara PTZ no puede ser utilizada por otras personas antes de ser liberada de forma manual o cuando el período ha expirado. El ajuste por defecto es de 1 hora. Si desea tiempos de espera en las cámaras individuales, se especifica esto en la pestaña **Posiciones predefinidas** para la cámara.
Ignorar los errores de comunicación del dispositivo si la comunicación restablecida antes	Seleccione por cuánto tiempo puede existir un error de comunicación antes de que el sistema lo registra como un error y dispara evento **error Comunicación**.

Los registros del servidor de la ficha (opciones)

En pestaña **Registros de servidores**, se puede especificar la configuración de los registros del servidor de gestión del sistema.

Consulte también Registros (explicados) (en la página 270) para obtener más información.

Nombre	Descripción
Registros	Seleccione el registro que desea configurar: • Registro del sistema • Registro de auditorías • Registro de reglas
Configuración	Activar / desactivar los registros y especifique el período de retención y el número máximo de filas para cada registro. Para registro del **Sistema**, especifique el nivel de los mensajes que desea iniciar sesión: • Todos - incluye mensajes no definidos • Información, advertencias y errores • Advertencias y errores • Los errores (configuración por defecto) Para los registros de **auditorías**, habilite el registro de acceso de usuario si desea que el sistema registre todas las acciones del usuario en XProtect Smart Client. Estos son, por ejemplo, las exportaciones, la activación de las salidas, cámaras de visualización en directo o en reproducción. Especificar: • la longitud de una secuencia de reproducción. Esto significa que mientras el usuario se reproduce dentro de este período, el sistema sólo genera una entrada en el registro. Cuando se reproducen fuera del período, el sistema crea una nueva entrada de registro. • el número de registros (frames) que un usuario ha visto antes de que el sistema crea una entrada de registro.

Pestaña Servidor de correo (opciones)

En la ficha **Servidor de correo**, puede especificar la configuración de servidor de correo SMTP saliente de su sistema.
Ver también Perfiles de notificación (explicados) (en la página 214).

Nombre	Descripción
Remitente del e-mail	Escriba la dirección de correo electrónico que desea que aparezca como remitente de las notificaciones de correo electrónico de todos los perfiles de notificación. Ejemplo: sender@organization.org.
El correo saliente (SMTP) nombre del servidor	Escriba el nombre del servidor de correo SMTP que envía notificaciones por correo electrónico. Ejemplo: mailserver.organization.org.

Nombre	Descripción
El servidor requiere datos de conexión	Especificar un nombre de usuario y la contraseña para los usuarios iniciar sesión en el servidor de correo.

Pestaña Generación AVI (opciones)

En la ficha **Generación de AVI**, puede especificar ajustes de compresión para la generación de archivos de video AVI. Se requieren los ajustes si desea incluir archivos AVI en las notificaciones de correo electrónico enviados por los perfiles de notificación de reglas por alarma.

Ver también Use reglas para desencadenar notificaciones por correo electrónico (ver "Utilizar reglas para desencadenar notificaciones por correo electrónico" en la página 215).

Nombre	Descripción
Compresor	Seleccione el códec (tecnología de compresión / descompresión) que desea aplicar. Para tener más códecs disponibles en la lista, instalarlas en el servidor de gestión. No todas las cámaras compatibles con todos los codecs.
La calidad de compresión	(No disponible para todos los codecs). Utilice el control deslizante para seleccionar el grado de compresión (**0** - **100**) a realizar por el codec. **0**significa que no hay compresión, lo que generalmente resulta en alta calidad de imagen y tamaño de archivo grande. **100** significa compresión máxima, por lo general resulta en una baja calidad de imagen y tamaño de archivo pequeño. Si el cursor no está disponible, la calidad de compresión se determina en su totalidad por el códec seleccionado.
Fotograma clave cada	(No disponible para todos los codecs). Si desea utilizar los fotogramas clave, seleccione la casilla de verificación y especifique el número necesario de fotogramas entre los fotogramas clave. Un fotograma clave es un solo cuadro almacenado en los intervalos especificados. El fotograma clave contiene toda la vista de la cámara, mientras que los siguientes cuadros contienen sólo los píxeles que cambian. Esto ayuda a reducir considerablemente el tamaño de los archivos. Si la casilla de verificación no está disponible, o no seleccionados, cada cuadro contiene toda la vista de la cámara.
Velocidad de datos	(No disponible para todos los codecs). Si desea utilizar una velocidad de datos en particular, seleccione la casilla de verificación y especifique el número de kilobytes por segundo. La velocidad de datos especifica el tamaño del archivo AVI adjunto. Si la casilla de verificación no está disponible, o no se selecciona, la velocidad de datos se determina por el códec seleccionado.

Pestaña Red (opciones)

En la ficha **Red**, puede especificar las direcciones IP de los clientes locales, si los clientes deben conectarse al servidor de grabación a través de Internet. El sistema de vigilancia entonces los reconoce como procedente de la red local.

También puede especificar la versión de IP del sistema: IPv4 o IPv6. El valor por defecto es IPv4.

Pestaña Favoritos (opciones)

Funcionalidad disponible depende del sistema que está utilizando. Ver tabla de comparación de productos (en la página 24) para más información.

En la ficha **Marcadores**, puede especificar los valores de los marcadores, sus documentos de identidad y la función de XProtect Smart Client.

Nombre	Descripción
Prefijo Identificación de marcadores	Especificar un prefijo para todos los marcadores que se hace por los usuarios de XProtect Smart Client.
Tiempo de marcador por defecto	Especifica la hora de inicio por defecto y al final de un favorito se encuentra en XProtect Smart Client. Este ajuste debe estar en consonancia con: • La regla de marcador por defecto, ver predeterminado de registros en regla marcador. • El período pre-buffer para cada cámara, ver Administrar pre-buffering (en la página 138).

Para especificar los derechos de marcador de un cometido, consulte derechos de Dispositivos (ver "Pestaña Dispositivo (cometidos)" en la página 251).

Pestaña configuración de usuario (opciones)

En la pestaña **Configuración del usuario**, puede especificar la configuración de preferencias del usuario, por ejemplo, si un mensaje se debe mostrar cuando se habilita la grabación remota.

Pestaña Customer Dashboard tab (opciones)

En la ficha **Customer Dashboard** se puede activar o desactivar Milestone Customer Dashboard.

Customer Dashboard es un servicio de monitoreo en línea que proporciona una visión general gráfica del estado actual de su sistema, incluyendo posibles problemas técnicos como fallos de cámara, administradores de sistemas u otras personas a las que se ha dado acceso a información sobre la instalación del sistema.

Puede seleccionar o desactivar la casilla de verificación para cambiar la configuración de Customer Dashboard en cualquier momento.

Pestaña Bloqueo de evidencias (opciones)

Funcionalidad disponible depende del sistema que está utilizando. Ver tabla de comparación de productos (en la página 24) para más información.

En la pestaña **Bloqueo de evidencias**, se definen y editar perfiles de bloqueo en la evidencia y la duración de sus usuarios del cliente puede seleccionar para mantener los datos protegidos.

Nombre	Descripción
Perfiles de bloqueo de evidencias	Una lista con los perfiles de bloqueo de evidencia definidos. Puede añadir y eliminar perfiles de bloqueo de evidencias existente. No se puede eliminar el perfil de bloqueo de evidencias por defecto pero puede cambiar sus opciones de tiempo y su nombre.
Opciones de tiempo de bloqueo	La duración de los usuarios del cliente puede seleccionar para bloquear pruebas. Las opciones de tiempo son hora (s), día (s), hora (s), mes (s), año (s), indefinida o definida por el usuario.

Para especificar los derechos de acceso de bloqueo de la evidencia de un cometido, consulte la ficha Dispositivo (ver "Pestaña Dispositivo (cometidos)" en la página 251) para la configuración de los cometidos.

Pestaña de mensajes de audio (opciones)

En la ficha **Mensajes de audio** , puede cargar archivos con mensajes de audio que se utilizan para difundir mensajes, activados por reglas.

El número máximo de archivos cargados es de 50 y el tamaño máximo permitido para cada archivo es de 1 MB.

Nombre	Descripción
Nombre	Proporciona el nombre de un mensaje.Introduzca el nombre cuando agregue un mensaje.Para cargar un mensaje en el sistema, haga clic en **Añadir** .
Descripción	Proporciona una descripción del mensaje. Introduzca la descripción cuando agregue un mensaje.Puede utilizar el campo de descripción para describir el propósito o el mensaje real.
Añadir	Permite cargar mensajes de audio en el sistema. Los formatos compatibles son formatos de archivo de audio estándar de Windows (.wav, .wma y .flac)
Editar	Permite modificar el nombre y la descripción, o puede reemplazar el archivo real.
Borrar	Elimine el mensaje de audio de la lista.
Jugar	Haga clic en este botón para escuchar el mensaje de audio desde el equipo que ejecuta el Management Client.

Para crear una regla que activa la reproducción de mensajes de audio, consulte . Agregue una regla (ver "Añadir una regla" en la página 208).

Para obtener más información sobre las acciones en general que puede utilizar en las reglas, consulte Acciones y acciones de detención (explicadas) (en la página 185).

Pestaña Configuración de control de acceso (opciones)

El uso de XProtect Access requiere que haya adquirido una licencia base que le permite acceder a esta función.

Nombre	Descripción
Mostrar panel de propiedades de desarrollo	Si se selecciona, aparece información adicional desarrollador para **Configuración de control de acceso> Generales** . Este ajuste sólo está destinado a ser utilizado por los desarrolladores de integraciones de sistemas de control de acceso.

Pestaña eventos analíticos (opciones)

En la pestaña **Eventos analíticos**, puede activar y especificar los análisis de eventos cuentan.

Nombre	Descripción
Habilitar	Especifique si desea utilizar los eventos analíticos. Por defecto, la función está desactivada.
Puerto	Especifique el puerto utilizado por esta característica. El puerto predeterminado es 9090. Asegúrese de que los proveedores de herramientas de VCA pertinentes también utilizan este número de puerto. Si cambia el número de puerto, recuerde que debe cambiar el número de puerto de los proveedores.
Todas las direcciones de red o direcciones de red especificado	Especificar si los eventos desde todas las direcciones IP / nombres de host se permite, o sólo los eventos de direcciones / nombres de host que se especifican en la **lista de direcciones** (véase más adelante) IP.
Lista de direcciones	Especificar una lista de direcciones IP / nombres de host de confianza. La lista filtra los datos entrantes de modo que / nombres de host solamente se permiten eventos desde determinadas direcciones IP. Se puede utilizar tanto Sistema de Nombres de Dominio (DNS), IPv4 e IPv6 formatos de dirección. Puede añadir direcciones a la lista introduciendo manualmente cada dirección IP o nombre de host, o mediante la importación de una lista externa de direcciones. • **Entrada manual:** Escriba la dirección IP / nombre en la lista de direcciones. Repita este procedimiento para cada dirección requerida. • **Importación:** Haga clic en **Importar** para buscar la lista externa de direcciones. La lista externa debe ser un archivo . txt y cada dirección IP o nombre de host debe estar en una línea separada.

Ficha Alarmas y eventos (opciones)

En la pestaña **Alarms and Events** , puede especificar ajustes para alarmas, eventos y registros (ver "Limitar el tamaño de la base de datos" en la página 64).

Nombre	Descripción
Mantenga cerradas las alarmas de	Especifique el número de días para almacenar alarmas con el estado **Cerrado** en la base de datos. Si ajusta el valor en **0** , la alarma se borra una vez cerrada. Las alarmas siempre tienen marcas de tiempo. Si la alarma se activa por una cámara, la marca de tiempo tiene una imagen de la hora de la alarma. La información de la alarma en sí se almacena en el servidor de eventos, mientras que las grabaciones de vídeo correspondientes a la imagen adjunta se almacenan en el servidor del sistema de vigilancia correspondiente. Para poder ver las imágenes de sus alarmas, mantenga las grabaciones de vídeo durante al menos el tiempo que usted tiene la intención de mantener las alarmas en el servidor de eventos.
Mantenga todas las otras alarmas de	Especifique el número de días para almacenar alarmas con el estado **Nuevo**, **En curso**, o **En espera**. Si ajusta el valor en 0, la alarma aparecerá en el sistema, pero no se almacenará. Las alarmas siempre tienen marcas de tiempo. Si la alarma se activa por una cámara, la marca de tiempo tiene una imagen de la hora de la alarma. La información de la alarma en sí se almacena en el servidor de eventos, mientras que las grabaciones de vídeo correspondientes a la imagen adjunta se almacenan en el servidor del sistema de vigilancia correspondiente. Para poder ver las imágenes de sus alarmas, mantenga las grabaciones de vídeo durante al menos el tiempo que usted tiene la intención de mantener las alarmas en el servidor de eventos.
Mantener los registros de	Especifique el número de días para guardar los registros del servidor de eventos. Si mantiene los registros durante períodos de tiempo más largos, asegúrese de que la máquina en la que está instalado el servidor de eventos tenga suficiente espacio en disco.
Habilitar el registro detallado	Para mantener un registro más detallado para la comunicación del servidor de eventos, seleccione la casilla de verificación. Se almacenará durante el número de días especificado en el **Guardar registros para el campo** .

Nombre	Descripción
Tipos de evento	Especifique el número de días para almacenar eventos en la base de datos. Hay dos maneras de hacer esto: • Puede especificar el tiempo de retención para todo un grupo de eventos. Los tipos de evento con el valor **Seguir el grupo** heredarán el valor del grupo de eventos. • Incluso si establece un valor para un grupo de eventos, puede especificar el tiempo de retención para tipos de eventos individuales. Si el valor es **0** , los eventos no se almacenarán en la base de datos. Los eventos externos (eventos definidos por el usuario, eventos genéricos y eventos de entrada) se establecen en **0** de forma predeterminada y no puede cambiar ese valor. La razón es que estos tipos de eventos ocurren con tanta frecuencia que almacenarlos en la base de datos puede causar problemas de rendimiento.

Pestaña eventos genéricas (opciones)

En la pestaña **Eventos Genéricos**, puede especificar eventos genéricos y los ajustes relacionados con la fuente de datos.

Para obtener más información acerca de cómo configurar eventos genéricos reales, consulte Eventos genéricos (explicado) (ver "Eventos genéricos (explicados)" en la página 223).

Nombre	Descripción
Fuente de datos	Se puede elegir entre dos fuentes de datos por defecto y definir una fuente de datos personalizada. ¿Qué a elegir depende de su programa de terceros y / o el hardware o software que desea interactuar a partir de: **Compatible:** Valores predeterminados de fábrica están activados, se hace eco de todos los bytes, TCP y UDP, sólo Ipv4, el puerto 1234, ningún separador, anfitrión local solamente, la página de códigos actual codificación (ANSI). **Internacional:** Valores predeterminados de fábrica están activados, se hace eco de estadísticas sólo, sólo TCP, Ipv4+6, el puerto 1235, <CR> <LF> como separador, anfitrión local solamente, codificación UTF-8. (<CR> <LF> = 13,10). [Fuente de C Datos] [Fuente de datos B] y así.
Nuevo	Haga clic para definir una nueva fuente de datos.
Nombre	Nombre del origen de datos.
Habilitado	Las fuentes de datos están habilitadas de forma predeterminada. Desactive la casilla de verificación para desactivar la fuente de datos.

Nombre	Descripción
restablecer	Haga clic para restablecer todos los ajustes para la fuente de datos seleccionada. El nombre introducido en el campo **Nombre** permanece.
Puerto	El número de puerto de la fuente de datos.
Selector de tipo de protocolo	Protocolos que el sistema debe escuchar a, y analizar, con el fin de detectar eventos genéricos: **Cualquier:** TCP, así como UDP. **TCP:** TCP solamente. **UDP:** UDP solamente. Paquetes TCP y UDP utilizados para eventos genéricos pueden contener caracteres especiales, como @, #, +, ~, y más.
selector de tipo IP	Seleccionables tipos de direcciones IP: IPv4, IPv6 o ambos.
Bytes separadoras	Seleccione los bytes de separación utilizados Para separar los registros de eventos genéricos individuales. Predeterminado para el tipo de fuente de datos **Internacional** (ver **Fuentes de datos** anterior) es **13,10**. (13,10 = <CR><IF>).
Selector del tipo de eco	Disponibles formatos de retorno del eco: • **Estadísticas de eco:** Se hace eco el siguiente formato: **[X], [Y], [Z], [Nombre del evento genérico]** **[X]** = número de solicitud. **[Y]** = número de caracteres. **[Z]** = número de partidos con un evento genérico. **[Nombre del evento genérico]** = nombre inscrito en el campo **Nombre**. • **Echo todos los bytes:** Se hace eco de todos los bytes. • **Sin eco:** Suprime todos los ecos.
Selector de tipo de codificación	Por defecto, la lista sólo muestra las opciones más relevantes. Seleccione la casilla verificación **Mostrar todo** para mostrar todas las codificaciones disponibles.
Las direcciones IPv4 externos permitidos	Especificar las direcciones IP, que el servidor de gestión debe ser capaz de comunicarse con el fin de gestionar los eventos externos. También puede usar esto para excluir direcciones IP que no desea datos.
Se admiten direcciones IPv6 externos	Especificar las direcciones IP, que el servidor de gestión debe ser capaz de comunicarse con el fin de gestionar los eventos externos. También puede usar esto para excluir direcciones IP que no desea datos.

Configuración de funciones

Servidores de gestión failover

Múltiples servidores de administración (agrupación) (explicado)

El servidor de gestión se puede instalar en varios servidores en un grupo de servidores. Esto asegura que el sistema tiene muy poco tiempo de inactividad. Si un servidor del clúster falla, otro servidor de la agrupación asume automáticamente el trabajo del servidor con el error que ejecuta el servidor de gestión. El proceso automático de conmutación del servicio de servidor para ejecutar en otro servidor de la agrupación sólo se tarda un tiempo muy corto (hasta 30 segundos).

Sólo es posible tener un servidor de gestión de configuración activo por la vigilancia, pero otros servidores de gestión se pueden configurar para asumir el control en caso de fallo.

El número permitido de failovers se limita a dos dentro de un período de seis horas. Si se excede, los servicios Management Server no se inician automáticamente por el servicio de agrupación. El número de conmutaciones permitidas se puede cambiar para adaptarse mejor a sus necesidades.

Requisitos para el agrupamiento

- Dos o más servidores instalados en un clúster:

  - Con respecto a los clústeres en MicrosoftWindows 2012®, consulte Clústeres de conmutación por error https://technet.microsoft.com/en-us/library/dn505754(v=ws.11).aspx.

- **De cualquier** una base de datos SQL externa instalada **fuera** el clúster de servidores **o** un servicio **interna** SQL (agrupado) dentro del clúster de servidores (la creación de un servicio de SQL interno requiere el uso de SQL Server Standard o una versión superior que es capaz de trabajar como un agrupado de SQL Server).

- A Microsoft® Windows® Servidor (Enterprise o edición de centro de datos).

Instalar en un clúster

Las descripciones e ilustraciones pueden diferir de lo que tu ves en la pantalla.

Instalación y cambio de dirección URL:

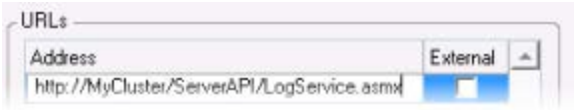
1. Instalar el servidor de gestión y todos sus subcomponentes en el primer servidor de la agrupación.

   El servidor de administración debe estar instalado con un usuario específico y no como un servicio de red **.** Esto requiere que utilice la **personalizada** opción de instalación **.**Además, el usuario específico debe tener acceso a la unidad de red compartida y, preferiblemente, una contraseña que no expire.

2. Después de haber instalado el servidor de administración y el Management Client en el primer servidor del clúster, abra el Management Client, y de menú **herramientas**, seleccionar **servicios registrados**.

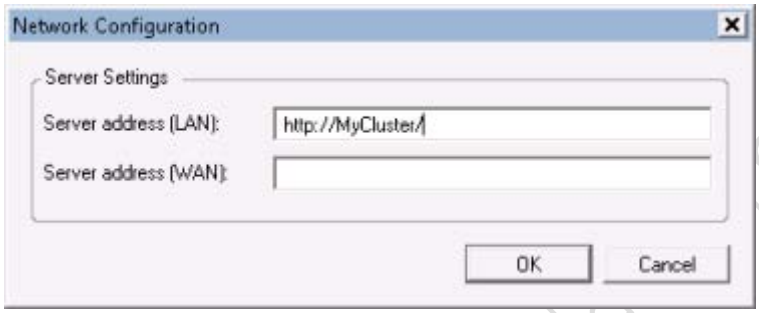
   1. En ventana **Añadir/borrar servicios registrados**, seleccione **Log Service** en la lista, haga clic en **Editar**.

2. En la ventana **Editar servicio registrada**, cambie la dirección URL del servicio de registro de la dirección URL del clúster.



3. Repita los pasos ayb para todos los servicios enumerados en la ventana **Añadir/borrar servicios registrados**. Haga clic **red**.

4. En la ventana **Configuración de red**, cambie la dirección URL del servidor a la dirección URL del clúster. (Este paso sólo se aplica al primer servidor de la agrupación.) Haga clic en **OK**.



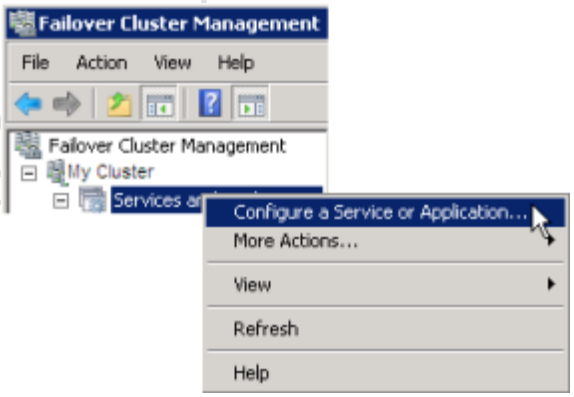
3. En la ventana **Añadir/borrar servicios registrados**, haga clic en **Cerrar**. Salir del Management Client.

4. Detener el servicio de servidor de gestión y el IIS. Lea acerca de cómo detener el IIS en la página de inicio de Microsoft® (http://technet.microsoft.com/en-us/library/cc732317(WS.10).aspx).

5. Repita los pasos 1-4 para todos los demás servidores de la agrupación, esta vez apuntando a la base de datos SQL existente. Sin embargo, para el **último** servidor en el clúster en el que se instala el servidor de gestión, no detener el servicio de servidor de gestión.

A continuación, con el fin de entrar en vigor, el servicio de administración de servidor debe estar configurado como un servicio genérico en el clúster failover:

1. En el último servidor en el que ha instalado el servidor de administración, vaya a **Inicio** > **Herramientas administrativas**, abierto **Administración de clúster de conmutación por error** de Windows. En la ventana **Administración de clúster de conmutación** expanda el clúster, haga clic **servicios y aplicaciones**, y seleccione **Configurar un servicio o aplicación**.



2. En el cuadro **alta disponibilidad** de diálogo haga clic en **Siguiente**, **Generic Service** y haga clic en **Siguiente**. No se especifica nada en la tercera página del cuadro de diálogo, haga clic en **Siguiente**.

3. Seleccione el **Milestone XProtect servidor de administración** servicio, haga clic en **Siguiente**. Especifique el nombre (nombre de host del clúster) que los clientes usan cuando se accede al servicio, haga clic en **Siguiente.**

4. No se requiere almacenamiento para el servicio, haga clic en **Siguiente**. Ninguna configuración del registro debe replicarse, haga clic en **Siguiente .**Compruebe que el servicio de clúster está configurado según sus necesidades, haga clic en **Siguiente .**El servidor de gestión está configurado como un servicio genérico en el clúster failover. Haga clic en **Finalizar**.

5. En la configuración de clúster, el servidor de eventos y el colector de datos deben establecerse como un servicio dependiente del servidor de gestión, por lo que el servidor de eventos se detiene cuando se detiene el servidor de gestión.

6. Para añadir el servicio **Milestone XProtect Event Server** como un recurso para la servicio de **Milestone XProtect Management Server Cluster**, haga clic en el servicio de clúster y haga clic **Añadir un recurso** > **4 - Servicio genérico** y seleccione **Milestone XProtect Event Server**.

Actualización de un clúster

Asegúrese de tener una copia de seguridad de la base de datos antes de actualizar el clúster.

1. Detener los servicios de servidor de gestión en todos los servidores de gestión del clúster.

2. Desinstalar el servidor de gestión en todos los servidores de la agrupación.

3. Utilice el procedimiento para instalar varios servidores de gestión de un clúster como se describe para instalar en un clúster, consulte Instalar en un clúster (en la página 293).

Importante: Durante la instalación, asegúrese de volver a utilizar la base de datos de configuración de SQL existente (que se actualiza automáticamente de la antigua versión de la base de datos existente a la nueva).

Servicios de conexión remota

Servicios de conexión remota (explicado)

Funcionalidad disponible depende del sistema que está utilizando. Ver tabla de comparación de productos (en la página 24) para más información.

La función de los servicios de conexión remota contiene la tecnología Axis One-click conexión del cámara desarrollado por Axis Communications. Se permite que el sistema para recuperar el vídeo (y audio) desde cámaras externas, donde los servidores de seguridad y / o enrutador de red configuración normalmente evita las conexiones de iniciación a este tipo de cámaras. La comunicación real se lleva a cabo a través de los servidores de túnel seguro (servidores ST). Servidores ST utilizan VPN. Sólo los dispositivos que poseen una obra clave válida dentro de una VPN. Esto ofrece un túnel seguro donde las redes públicas pueden intercambiar datos de forma segura.

Conectar a distancia de servicios le permite:

- Editar credenciales dentro del Servicio Axis Dispatch Service
- Añadir, editar y eliminar servidores ST
- Registrar/anular y editar Axis One-click cámaras

- Ir al hardware relacionado con el cámara Axis One-Click.

Antes de poder utilizar Axis One-click Camera Connection de un solo clic, primero debe instalar un entorno adecuado servidor ST. Para trabajar con el servidor (ST) entornos de servidores túnel seguro y con Axis One-click cámaras, primero debe ponerse en contacto con el proveedor del sistema para obtener el nombre de usuario y la contraseña necesaria para Axis Dispatch Services.

Instalar STS entorno de conexión de la cámara de un solo clic

Requisitos

- Póngase en contacto con el proveedor del sistema para obtener el nombre de usuario y la contraseña necesaria para Axis Dispatch Services.
- Asegúrese de que su cámara(s) de apoyo Axis Video Hosting System. Ir a la página web Axis para ver los dispositivos compatibles (http://axis-avhs.com/supported-devices/).
- Si es necesario, actualizar sus cámaras Axis con el nuevo firmware. Ir a la página web Axis para descargar el firmware (http://www.axis.com/techsup/firmware.php).

1. En la página principal de cada cámara, vaya a **Configuración básica**, **TCP / IP**, y seleccione **Habilitar AVHS** y **Siempre**.
2. Desde su servidor de gestión, vaya a la Milestone página de descarga (http://www.milestonesys.com/downloads) y descargue **AXIS One-click** software. Ejecute el programa para configurar un Axis secure tunnel framework. adecuado.

Añadir / editar los SPB

1. Puede seguir estos pasos:
    1. Para añadir un servidor ST, haga clic en nodo superior de **Axis Secure Tunnel Servers**, seleccione **Add Axis Secure Tunnel Server**.
    2. Para editar un servidor ST, haga clic en él, seleccione **Editar servidor de túnel seguro Axis**.
2. En la ventana que se abre, rellene la información relevante.
3. Si decide utilizar credenciales al instalar el **Axis One-Click componente de conexión**, seleccione la casilla de verificación **Usar credenciales** y rellenar el mismo nombre de usuario y contraseña que se utiliza para la **Axis One-Click componente de conexión**.
4. **Haga clic en OK (aceptar)**.

Registrar nueva cámara Axis One-Click

1. Para registrar una cámara bajo un servidor ST, haga clic en él y seleccione **Registro Axis One-Click cámara**.
2. En la ventana que se abre, rellene la información relevante.
3. **Haga clic en OK (aceptar)**.
4. La cámara ahora aparece en el servidor relevante ST.

La cámara puede tener la siguiente codificación de color:

Color	Descripción
Rojo	Estado inicial. Registrado, pero no está conectado al servidor ST.
Amarillo	Registrado. Conectado al servidor ST, pero no se añade como hardware.
Verde	Agregado como hardware. Puede o no puede conectarse al servidor ST.

Cuando se agrega una nueva cámara, su estado es siempre verde. El estado de la conexión se refleja **Dispositivos** en **Servidores de grabación** en el **Visión de conjunto** panel. En el **Visión de conjunto** panel, puede agrupar sus cámaras para obtener una visión general más fácil. Si tu eliges **no** para registrar su cámara en el servicio de envío de Axis en este momento, puede hacerlo más adelante desde el menú del botón derecho del ratón (seleccione **Editar cámara Axis One-Click**).

Axis One-Click propiedades de conexión de la cámara

Nombre	Descripción
Contraseña de la cámara	Introducir / editar. Proporciona con la cámara en la compra. Para más detalles, consulte el manual de su cámara o ir a la página web de Axis (http://www.axis.com).
Usuario de la cámara	Ver detalles de la **contraseña cámara**.
Descripción	Introducir / editar una descripción para la cámara.
Dirección externa	Introducir / editar la dirección http del servidor ST a la que la cámara (s) conectar.
Dirección interna	Introducir / editar la dirección http del servidor ST al que se conecta el servidor de grabación.
Nombre	Si es necesario, edite el nombre del elemento.
Clave de autenticación propietario	Ver **contraseña cámara**.
Contraseñas (por Dispatch Server)	Introducir la contraseña. Debe ser idéntica a la información recibida desde el proveedor del sistema.
Contraseñas (para el servidor ST)	Introducir la contraseña. Debe ser idéntico al que se especificado cuando el **Axis One-Click Connection Component** se instaló .
Registrarse / Anular registro en el Servicio de Despacho del Eje	Indique si desea registrar su cámara Axis con el servicio Axis dispatch. Se puede hacer en el momento de la instalación o después.
Número de serie	Número de serie del hardware según lo especificado por el fabricante. El número de serie es a menudo, pero no siempre, idéntica a la dirección MAC.
Usar credenciales	Seleccione la casilla de verificación si ha decidido usar las credenciales durante la instalación del servidor ST.
Nombre de usuario (para Dispatch Server)	Introduzca un nombre de usuario. El nombre de usuario debe ser idéntica a la recibida de su proveedor de sistema.

Nombre de usuario (para el servidor ST)	Introduzca su nombre de usuario. Debe ser idéntico al que se especificado cuando el **Axis One-Click Connection Component** se instaló .

Milestone Federated Architecture

Seleccionando Milestone Interconnect o Milestone Federated Architecture (explicado)

En un sistema físicamente distribuido donde los usuarios del sitio central necesitan acceder al video en el sitio remoto, puede elegir entre Milestone Interconnect™ o Milestone Federated Architecture™.

Milestone recomienda Milestone Federated Architecture cuando:

- La conexión de red entre los sitios centrales y federados es estable.
- La red utiliza el mismo dominio.
- Hay menos sitios más grandes.
- El ancho de banda es suficiente para el uso requerido.

Milestone recomienda Milestone Interconnect cuando:

- La conexión de red entre los sitios centrales y remotas es inestable.
- Usted o su organización desea utilizar otro producto XProtect en los sitios remotos.
- La red utiliza diferentes dominios o grupos de trabajo.
- Hay muchos sitios más pequeños.

Milestone Federated Architecture (explicado)

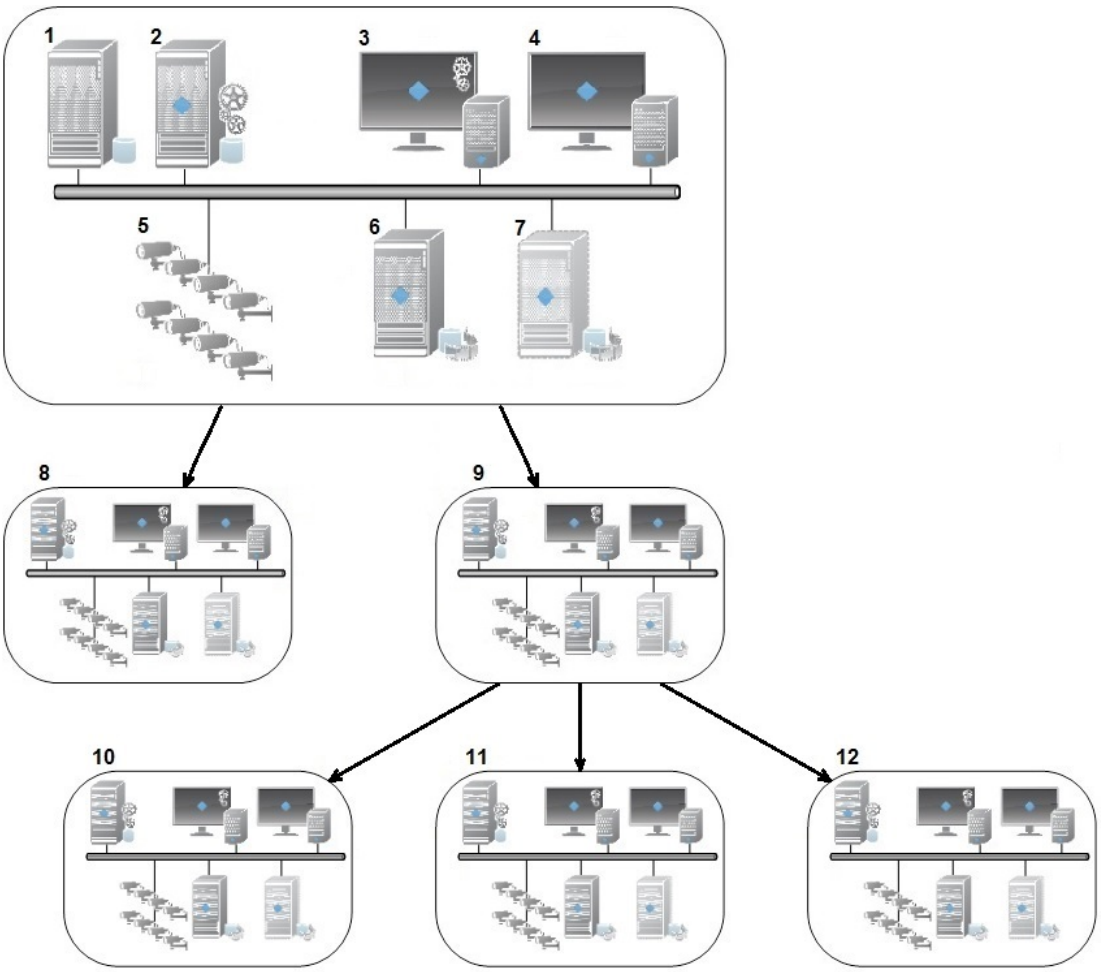
Funcionalidad disponible depende del sistema que está utilizando. Ver tabla de comparación de productos (en la página 24) para más información.

Milestone Federated Architecture vincula múltiples sistemas estándar individuo en una jerarquía de sitios federados de sitios principales / secundarios. Los usuarios de clientes con derechos suficientes tienen acceso transparente a vídeo, audio y otros recursos a través de los sitios individuales. Los administradores pueden administrar de forma centralizada todos los sitios dentro de la jerarquía federada, en función de los derechos de administrador de los sitios individuales.

Los usuarios básicos no son compatibles con los sistemas Milestone Federated Architecture, por lo que debe añadir usuarios como usuarios de Windows a través del servicio de Active Directory.

Importante: Desde el Management Client, puede administrar de forma centralizada los sitios federados que ejecutan versiones anteriores del producto después de que corrigen los servidores .Las versiones compatibles son XProtect Corporate 2014 y XProtect Expert 2014 o posterior.

Milestone Federated Architecture está configurado con un sitio central (sitio superior) y un número sin restricciones de sitios federados (ver "Configurar su sistema para ejecutar sitios federados" en la página 301).Cuando se inicia la sesión en un sitio web, puede acceder a información sobre todos sus sitios secundarios y sitios secundarios de los sitios secundarios. El vínculo entre dos sitios se establece, cuando usted solicitar el enlace desde el sitio principal (ver "Añadir sitio a la jerarquía" en la página 303). Un sitio secundario sólo puede estar vinculado a un sitio principal. Si no es el administrador del sitio secundario cuando se agrega a la jerarquía del sitio federado, la petición debe ser aceptada por el administrador del sitio secundario.



Los componentes de una configuración Milestone Federated Architecture:

1. SQL server
2. Servidor de gestión
3. Management Client
4. XProtect Smart Client
5. Cámaras
6. Servidor de grabación
7. Servidor de grabación failover
8. a 12. sitios federados

Sincronización de jerarquía

Un sitio principal contiene una lista actualizada de todos sus sitios secundarios conectados actualmente, los sitios secundarios, sitios secundarios de sitios secundarios y así sucesivamente. La jerarquía de sitios federados tiene una sincronización programada entre los sitios, así como la sincronización de gestión activado por cada vez que se añade o elimina un sitio. Cuando el sistema se sincroniza la jerarquía, se necesita nivel lugar por nivel, cada nivel de reenvío y la comunicación de regresar, hasta que llega al servidor que solicita la información. El sistema envía menos de 1 MB cada vez. Dependiendo del número de niveles, los cambios en una jerarquía pueden tomar algún tiempo para llegar a ser visible en el Management Client. No se puede programar sus propias sincronizaciones.

Tráfico de datos

El sistema envía los datos de comunicación o de configuración cuando un usuario ve o administrador directo o vídeo grabado o configura un sitio. La cantidad de datos depende de qué y cuánto se está viendo o configure.

Milestone Federated Architecture con otros productos

- Si el sitio central utiliza XProtect Smart Wall, también puede utilizar las funciones Smart Wall en la jerarquía de sitios federados. Consulte Configure Smart Wall s (ver "Configurar Smart Walls" en la página 323) en cómo configurar un Smart Wall.
- Si el sitio central utiliza XProtect Access y un XProtect Smart Client el usuario inicia sesión en un sitio en una jerarquía de sitio federado, las notificaciones de solicitud de acceso de los sitios federados también aparecen en XProtect Smart Client.
- Puede añadir sistemas XProtect Expert 2013 o más recientes a la jerarquía de sitios federados como sitios secundarios, no como sitios primarios.
- Milestone Federated Architecture no requiere licencias adicionales.
- Para obtener más información acerca de los casos de uso y los beneficios, vea el documento acerca de la tecnología de Milestone Federated Architecture en el sitio web de Milestone.
- Para integrar XProtect Professional VMS 7.0 y superior en su sistema, consulte XProtect Professional VMS servidores (explicado) (ver "Servidores XProtect Professional VMS (explicados)" en la página 440).

El establecimiento de una jerarquía de sitios federados

Antes de comenzar la construcción de la jerarquía del Management Client, Milestone recomienda que asigne cómo desea que sus sitios se enlazan entre sí.

Instalar y configurar cada sitio en una jerarquía federada como un sistema autónomo normal con componentes estándar del sistema, configuración, reglas, horarios, administradores, usuarios y derechos de usuario. Si ya dispone de los sitios instalados y configurados y sólo necesita para combinarlos en una jerarquía de sitios federados, sus sistemas están listos para ser establecido.

Una vez que los sitios individuales están instalados, debe configurarlos para que se ejecuten como sitios federados (ver "Configurar su sistema para ejecutar sitios federados" en la página 301).

Para iniciar la jerarquía, puede iniciar sesión en el sitio que desea trabajar como el sitio central y añadir (ver "Añadir sitio a la jerarquía" en la página 303) el primer sitio federado. Cuando se establece el enlace, los dos sitios crean automáticamente una jerarquía de sitios federados en el panel **Jerarquía de sitios Federados** en el Management Client al que se pueden añadir más sitios a crecer la jerarquía federada.

Cuando haya creado una jerarquía de sitios federada, los usuarios y los administradores pueden iniciar sesión en un sitio para acceder a ese sitio y todos los sitios federados que pueda tener. El acceso a los sitios federados dependen de los derechos de los usuarios.

No hay límite en el número de sitios que se pueden añadir a la jerarquía federada. También, usted puede tener un sitio en una versión más antigua de productos vinculados a una versión más nueva y viceversa. Los números de versión aparecen de forma automática y no se pueden borrar. El sitio que ha iniciado sesión en está siempre en la parte superior del panel **Jerarquía de sitios federados** y se llama sitio de la casa.

Ejemplo de sitios federados del Management Client
A la izquierda: Iniciado sesión en el sitio de la parte superior.
A la derecha: Iniciado sesión en uno de los sitios secundarios. En este ejemplo, el servidor de París, que es entonces el sitio de la casa.

Los iconos de estado en Milestone Federated Architecture

Los iconos representan los posibles estados de un sitio:

Descripción	Icono
El sitio de la parte superior en la jerarquía está en funcionamiento.	
El sitio de la parte superior en la jerarquía completa está todavía en funcionamiento, pero uno o más problemas que necesitan atención. Se muestra en la parte superior del icono del sitio superior.	
El sitio está en funcionamiento.	
El sitio está a la espera de ser aceptado en la jerarquía.	
El sitio es la fijación, pero aún no está en funcionamiento.	

Configurar su sistema para ejecutar sitios federados

Para preparar su sistema para Milestone Federated Architecture, debe tomar ciertas decisiones al instalar el servidor de gestión. Dependiendo de cómo la infraestructura de TI está configurada, elegir entre tres alternativas diferentes.

Alternativa 1: Conectar sitios desde el mismo dominio (con un usuario de dominio común)

Antes de instalar el servidor de gestión, debe crear un usuario de dominio común y configurar este usuario como administrador en todos los servidores que participan en la jerarquía del sitio federado.

Instalación personalizada

1. Iniciar la instalación del producto en el servidor para ser utilizado como servidor de gestión y seleccione **Personalizada**.

2. Seleccionar para instalar el servicio de Management Server utilizando una cuenta de usuario. La cuenta de usuario seleccionada debe ser la cuenta del administrador usada en todos los servidores de gestión. Debe utilizar la misma cuenta de usuario al instalar los otros servidores de gestión en la jerarquía del sitio federado.

3. Finalizar la instalación. Repita los pasos 1-3 para instalar cualquier otro sistema que desee añadir a la jerarquía de sitios federados.

4. Añadir sitio a jerarquía (ver "Añadir sitio a la jerarquía" en la página 303).

Único equipo o Instalación distribuida: configure el servicio de red en todos los servidores

1. Inicie la instalación del producto en el primer servidor que se utilizará como servidor de gestión y seleccione **Único equipo** o **Distribuido**. Esto instala el servidor de gestión con una cuenta de servicio de red. Repita este paso para todos los sitios de la jerarquía de sitios federados.

2. Iniciar sesión en el sitio que desea que el sitio central en la jerarquía del sitio federado.

3. En el Management Client, expanda **Seguridad** > **Cometidos** > **Administradores**.

4. En la ficha **Usuarios y grupos**, haga clic en **Añadir** y seleccione **Usuario de Windows**.

5. En el cuadro de diálogo, seleccione **Computadoras** como tipo de objeto, escriba el nombre del servidor del sitio federado y haga clic en **Aceptar** para añadir el servidor a la función **Administrador** del sitio central. Repita este paso hasta que haya agregado todos los sitios federados en este camino y salir de la aplicación.

6. Iniciar sesión en cada sitio federados, y añadir los siguientes servidores para el cometido de **Administrador**, de la misma manera que el anterior:

   - El servidor del sitio principal.
   - Los servidores de sitio secundario que desea conectarse directamente a este sitio federados.

7. Añadir sitio a jerarquía (ver "Añadir sitio a la jerarquía" en la página 303).

Alternativa 2: Los sitios de unión de diferentes dominios

Para conectarse a sitios a través de dominios, asegúrese de que los dominios confían entre sí. Se configura dominios a confiar entre sí en la configuración del dominio de Microsoft Windows. Cuando haya establecido la confianza entre los diferentes dominios en cada sitio en la jerarquía de sitios federados, siga la misma descripción que se describe en la alternativa 1. Para obtener más información acerca de cómo configurar dominios de confianza, consulte el sitio web de Microsoft (http://technet.microsoft.com/en-us/library/cc961481.aspx).

Milestone recomienda Milestone Interconnect para la creación de sistemas de múltiples sitios conectados con múltiples dominios.

Alternativa 3: Conectar los sitios de grupo(s) de trabajo

Cuando conecta sitios dentro de grupos de trabajo, la misma cuenta de administrador debe estar presente en todos los servidores que desee conectar en la jerarquía de sitios federados. Debe definir la cuenta de administrador antes de instalar el sistema.

1. Iniciar sesión en **Windows** utilizando una cuenta de administrador común.

2. Iniciar la instalación del producto y haga clic **Personalizada**.

3. Seleccionar para instalar el servicio Management Server utilizando la cuenta de administrador común.
4. Finalizar la instalación. Repita los pasos 1-4 para instalar cualquier otro sistema que desee conectar. Debe instalar todos estos sistemas utilizando la cuenta de administrador común.
5. Añadir sitio a jerarquía (ver "Añadir sitio a la jerarquía" en la página 303).

Milestone recomienda Milestone Interconnect para la creación de sistemas de múltiples sitios conectados cuando los sitios no son parte de un dominio.

No se puede mezclar dominio(s) y grupo(s) de trabajo. Esto significa que no se puede conectar sitios de un dominio a los sitios de un grupo de trabajo y viceversa.

Añadir sitio a la jerarquía

A medida que expande su sistema, puede añadir sitios a su sitio arriba y para sus sitios secundarios siempre y cuando el sistema está configurado correctamente.

1. Seleccione panel **Jerarquía de sitios Federados**.
2. Seleccione el sitio al que desea añadir un sitio secundario, haga clic en y haga clic en **Añadir Sitio a Jerarquía**.
3. Introduzca la URL de la página solicitada en el sitio **Añadir a la jerarquía** ventana y haga clic en **OK**.
4. El sitio principal envía una petición de enlace para el sitio secundario y después de un tiempo, se agregó un enlace entre los dos sitios al panel **Jerarquía de sitios Federados**.
5. Si puede establecer el enlace al sitio secundario sin solicitar la aceptación del administrador del sitio secundario, vaya al paso 7.

   Si **no**, el sitio secundario tiene la aceptación pendiente hasta que el administrador del sitio secundario haya autorizado la solicitud.
6. Asegúrese de que el administrador del sitio secundario autoriza la petición de enlace desde el sitio primario (ver "Aceptar su inclusión en la jerarquía" en la página 303).
7. El nuevo vínculo padre / hijo se establece y el panel **Jerarquía de sitios federados** se actualiza con el icono para el nuevo sitio secundario.

Aceptar su inclusión en la jerarquía

Cuando un sitio secundario ha recibido una solicitud de enlace de un sitio principal potencial donde el administrador no tenía derechos de administrador al sitio secundario, tiene la aceptación pendiente icono.

Para aceptar una solicitud de enlace:

1. Iniciar sesión en el sitio.
2. En el panel **Jerarquía de sitios federados**, haga clic en el sitio y haga clic en **Aceptar inclusión en la jerarquía**.

   Si el sitio ejecuta la versión XProtect Expert, haga clic con el botón secundario en el sitio en el panel **Navegación del sitio**.
3. Haga clic en **Sí**.

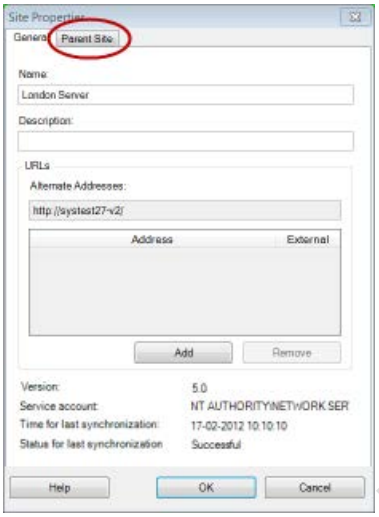
4. El nuevo vínculo padre / hijo se establece y el panel **Jerarquía de sitios federados** se actualiza con el sitio normal icono para el sitio seleccionado.

Los cambios que realice en los sitios secundarios situados lejos del sitio principal puede tardar algún tiempo en reflejarse en el panel **Jerarquía de sitios Federados**.

Establecer las propiedades del sitio

Puede ver y, posiblemente, editar propiedades en su sitio de la casa y sus sitios secundarios.

1. En el Management Client, en el panel **Jerarquía de sitios federados**, seleccione el sitio relevante, haga clic con el botón secundario del mouse y seleccione **Propiedades**.



2. Si es necesario, cambie lo siguiente:

   Pestaña **General** (en la página 305)

   Pestaña **Página principal** (ver "Pestaña Sitio principal" en la página 306)(**disponible sólo en sitios secundarios)**

Debido a problemas de sincronización, los cambios realizados a los sitios secundarios remotas pueden tardar algún tiempo en reflejarse en el panel de **navegación del sitio**.

Actualizar la información de sitio

Esta sección sólo es relevante si utiliza XProtect Corporate o XProtect Expert 2014 o posterior.

Puede leer la información sobre el sitio, al poner el ratón sobre el nombre del sitio en el panel de la **Jerarquía de sitios federados**. Para actualizar la información de la página:

1. Iniciar sesión en el sitio.
2. Haga clic **Navegación en el sitio** panel y seleccione **Información del sitio**.
3. Haga clic en **Editar** y añadir la información relevante en cada categoría.

Actualización de jerarquía de sitios

Regularmente el sistema sincroniza automáticamente la jerarquía a través de todos los niveles de la configuración de su principal / secundario. Puede actualizar manualmente, si desea ver los cambios reflejados instantáneamente en la jerarquía, y no desea esperar a la siguiente sincronización automática.

Es necesario estar conectado en un sitio para llevar a cabo una actualización manual. Sólo los cambios guardados por este sitio desde la última sincronización se reflejan por un refresco. Esto significa que los cambios realizados más abajo en la jerarquía no pueden ser reflejados por la actualización manual, si los cambios no han alcanzado aún el sitio.

1. Iniciar sesión en el sitio pertinente.
2. Haga clic en el sitio superior en el panel **Jerarquía de sitios Federados** y haga clic en **Actualizar Jerarquía de sitios**.

   Esto tomará unos segundos.

Iniciar sesión en otros sitios de la jerarquía

Puede iniciar sesión en otros sitios y administrar estos. El sitio al que está conectado a su sitio es el hogar.

1. En el panel **Jerarquía de sitios federados**, haga clic con el botón secundario en el sitio en el que desea iniciar sesión.
2. Haga clic en **Iniciar sitio**.

   El Management Client para ese sitio se abre.
3. Introduzca la información de acceso y haga clic en **OK**.
4. Después de conexión esté completo, usted está listo para hacer sus tareas administrativas para ese sitio.

Separar un sitio de la jerarquía

Al separar un sitio de su sitio primario, el enlace entre los sitios están rotas. Puede separar los sitios desde el sitio central, desde el mismo sitio o su 'sitio principal.

1. En el panel **Jerarquía de sitios federados**, haga clic en el sitio, y haga clic en **Desasociar sitio de la jerarquía**.
2. Haga clic en **Sí** para actualizar el panel **Jerarquía de sitio federado**.

   Si el sitio separado tiene sitios secundarios, se convierte en el nuevo sitio superior para esta rama de la jerarquía y el icono de sitio normal cambios en un sitio superior icono.
3. **Haga clic en OK (aceptar)**.

Los cambios en la jerarquía se reflejan después de una actualización manual o una sincronización automática.

Propiedades del sitio federados

Pestaña General

Puede cambiar algo de la información relacionada con el sitio al que está conectado actualmente a.

Nombre	Descripción
Nombre	Introduzca el nombre del sitio.
Descripción	Introduzca una descripción del sitio.
URL	Utilice la lista para añadir y quitar URL (s) de este sitio e indicar si son externos y no. Direcciones externas se puede acceder desde fuera de la red local.
Versión	El número de versión del servidor de gestión del sitio.
Cuenta de servicio	La cuenta de servicio con la que el servidor de gestión se está ejecutando.
La hora de la última sincronización	Hora y fecha de la última sincronización de la jerarquía.
Estado para la última sincronización	El estado de la última sincronización de la jerarquía. Puede ser **Con éxito** o **Fallo**.

Pestaña Sitio principal

Esta pestaña muestra información sobre el sitio principal del sitio que está conectado actualmente a. La ficha no es visible si su sitio no tiene sitio principal.

Nombre	Descripción
Nombre	Muestra el nombre del sitio primario.
Descripción	Muestra una descripción del sitio primario (opcional).
URL	Listas de URL (s) para el sitio principal e indica si son o no externa. Direcciones externas se puede acceder desde fuera de la red local.
Versión	El número de versión del servidor de gestión del sitio.
Cuenta de servicio	La cuenta de servicio con la que el servidor de gestión se está ejecutando.
La hora de la última sincronización	Hora y fecha de la última sincronización de la jerarquía.
Estado para la última sincronización	El estado de la última sincronización de la jerarquía. Puede ser **Con éxito** o **Fallo**.

Milestone Interconnect

Seleccionando Milestone Interconnect o Milestone Federated Architecture (explicado)

En un sistema físicamente distribuido donde los usuarios del sitio central necesitan acceder al video en el sitio remoto, puede elegir entre Milestone Interconnect™ o Milestone Federated Architecture™.

Milestone recomienda Milestone Federated Architecture cuando:

- La conexión de red entre los sitios centrales y federados es estable.
- La red utiliza el mismo dominio.
- Hay menos sitios más grandes.
- El ancho de banda es suficiente para el uso requerido.

Milestone recomienda Milestone Interconnect cuando:

- La conexión de red entre los sitios centrales y remotas es inestable.
- Usted o su organización desea utilizar otro producto XProtect en los sitios remotos.
- La red utiliza diferentes dominios o grupos de trabajo.
- Hay muchos sitios más pequeños.

Seleccione un plan para las API de Google Maps o Bing Maps

Bing Maps y Google Maps ofrecen diferentes planes de uso para sus APIs. Cuando selecciona un plan es importante considerar cuánto usará el servicio de mapas.

Bing Maps ofrece claves básicas y claves empresariales, y Google Maps ofrece planes estándar y Premium. Las claves básicas para Bing Maps son gratuitas, pero permiten un número limitado de transacciones antes de que las transacciones se conviertan en facturables o se deniegue el acceso al servicio de mapas. Las claves Premium y Enterprise no son gratuitas, pero permiten transacciones ilimitadas.

Si va a utilizar Bing Maps o Google Maps en XProtect Smart Client, Milestone recomienda lo siguiente:

- Para Bing Maps, compre una clave de empresa. También puede utilizar una clave básica, pero recuerde que permiten un uso limitado.
- Para utilizar Google Maps, debe adquirir un Plan Premium para la API de Google Static Maps.

Para obtener más información, visite los siguientes sitios web:

- Mapas de Bing (https://www.microsoft.com/maps/Licensing/licensing.aspx)
- Consola para desarrolladores de Google Maps (https://developers.google.com/maps/pricing-and-plans/)

Siguiente, Ingrese la clave de Bing Maps o la clave de Google Maps o el ID de cliente en Management Client (en la página 317).

Milestone Interconnect y concesión de licencias

Para ejecutar Milestone Interconnect, necesita licencias de cámara de Milestone Interconnect en su sitio central para ver el vídeo de los dispositivos de hardware en sitios remotos. Tenga en cuenta que XProtect Corporate como instalación central.

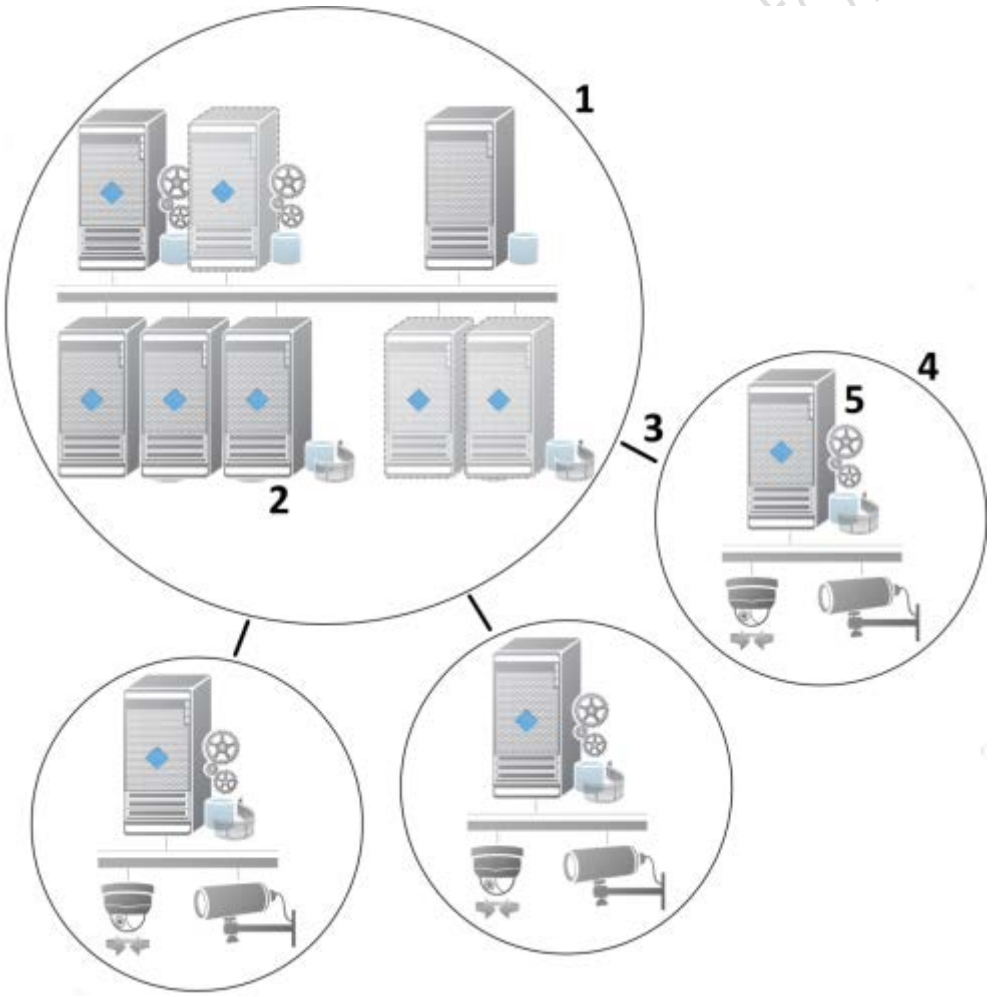
El estado de sus licencias de cámara de Milestone Interconnect están listados en la **información de licencia** página del sitio central.

Milestone Interconnect (explicado)

Funcionalidad disponible depende del sistema que está utilizando. Ver tabla de comparación de productos (en la página 24) para más información.

Milestone Interconnect™ le permite integrar una serie de más pequeño, físicamente fragmentada, y la distancia XProtect o Milestone Husky™ NVR instalaciones con un solo XProtect Corporate sitio central. Puede instalar estos sitios más pequeños, llamados sitios remotos, en unidades móviles, por ejemplo, barcos, autobuses o trenes. Esto significa que tales sitios no necesitan estar permanentemente conectados a una red.

La siguiente ilustración muestra cómo se puede configurar Milestone Interconnect en el sistema:



1. Milestone Interconnect sistema central de XProtect Corporate

2. Controladores de Milestone Interconnect (se encarga de la conexión entre servidores de grabación de los sitios centrales y el sitio remoto, se deben seleccionar en la lista de controladores al añadir sistemas remotos a través de la asistente **Añadir hardware**)
3. La conexión de Milestone Interconnect
4. Sitio remoto Milestone Interconnect (el sitio remoto completa con la instalación del sistema, los usuarios, las cámaras y así sucesivamente)
5. Sistema remoto de Milestone Interconnect (la instalación técnica efectiva en el sitio remoto)

Agrega sitios remotos a su sitio central con el asistente **Añadir hardware** desde el sitio central (ver "Añadir un sitio remoto a su sitio central de Milestone Interconnect" en la página 310).

Cada sitio remoto se ejecuta de forma independiente y se puede realizar ninguna tarea de vigilancia normales. Dependiendo de las conexiones de red y de los derechos de usuario (ver "Asignar derechos de usuario" en la página 311) adecuados, Milestone Interconnect le ofrece la visualización en directo directa de cámaras de sitios remotos y la reproducción de grabaciones de sitios remotos en el sitio central.

El sitio central sólo puede ver y dispositivos de acceso que la cuenta de usuario especificada (cuando se agrega el sitio remoto) tiene acceso a. Esto permite a los administradores de sistemas locales para controlar los dispositivos que puedan estar a disposición en el sitio central y sus usuarios.

En el sitio central, puede ver el estado del propio sistema de las cámaras interconectadas, pero no directamente el estado de sitio remoto. En cambio, para vigilar el sitio remoto, puede utilizar las eventos del sitio remoto para activar alarmas u otras notificaciones en el sitio central (ver "Configurar su sitio central para responder a eventos desde sitios remotos" en la página 313).

También le ofrece la posibilidad de transferir las grabaciones de sitio remoto al sitio central, ya sea basado en eventos, reglas / horarios, o solicitudes manuales de usuarios XProtect Smart Client.

Sólo los sistemas XProtect Corporate pueden funcionar como lugares centrales. Todos los demás productos pueden actuar como sitios remotos, incluyendo XProtect Corporate. Se diferencia de la configuración para configurar qué versiones, el número de cámaras, y cómo los dispositivos y eventos que se originan desde el sitio remoto se manejan - en todo caso - por el sitio central. Para obtener más información sobre cómo interactúan los productos XProtect específicos en una instalación Milestone Interconnect, vaya al sitio web (http://www.milestonesys.com/our-products/milestone-interconnect/) Milestone Interconnect.

Milestone Interconnect configuraciones (explicado)

Hay tres maneras de ejecutar Milestone Interconnect. Cómo ejecutar la configuración depende de su conexión de red, cómo reproducir las grabaciones, y si se recupera grabaciones remotas y en qué grado.

En lo que sigue, se describen las tres configuraciones más probables:

La reproducción directa desde sitios remotos (conexiones de red buena)

La configuración más sencilla. El sitio central está continuamente en línea con sus sitios remotos y los usuarios de sitio central reproducir grabaciones remotas directamente desde los sitios remotos. Esto requiere el uso de la opción **Reproducción de grabaciones del sistema remoto** (ver "**Habilitar la reproducción directamente desde el sitio remoto de la cámara**" en la página 312).

La recuperación basada en el XProtect Smart Client o en reglas de secuencias de grabación remotos seleccionados desde sitios remotos (limitado periódicamente las conexiones de red)

Se utiliza cuando las secuencias de grabación seleccionados (procedente de emplazamientos remotos) deben almacenarse de forma centralizada para garantizar la independencia de los sitios remotos. La independencia es

crucial en caso de fallo en la red o restricciones de la red. Configurar los valores de las grabaciones de recuperación remota en la pestaña **recuperación remota** (en la página 119).

Grabaciones de recuperación remota se puede iniciar desde el XProtect Smart Client cuando sea necesario o una regla se puede configurar. En algunos casos, los sitios remotos están en línea y en otros, fuera de línea la mayor parte del tiempo. Esto es a menudo específico de la industria. Para algunas industrias es común que el sitio central que esté permanentemente conectado con sus sitios remotos (por ejemplo, un HQ al por menor (sitio central) y un número de tiendas (sitios remotos)). Para otros sectores, como el transporte, los sitios remotos son móviles (por ejemplo, autobuses, trenes, barcos, etc.) y sólo se puede establecer una conexión de red al azar. En caso de fallar la conexión de red durante una recuperación comenzado la grabación remota, la tarea continúa en la próxima oportunidad dada.

Si el sistema detecta una recuperación automática o una solicitud de recuperación desde XProtect Smart Client, fuera del intervalo de tiempo que especificó en la ficha **Recuperación remota**, se acepta, pero no se inicia hasta que se alcanza el intervalo de tiempo seleccionado. Los nuevos trabajos de recuperación de grabación remota pondrán en cola y empezar cuando se alcanza el intervalo de tiempo permitido. Puede ver los trabajos de recuperación de la grabación remotas pendientes desde **Panel de sistema** -> **Tareas actuales**.

Después de un fallo de conexión, grabaciones remotas que faltan se recuperan de forma predeterminada desde sitios remotos

Utiliza sitios remotos como un servidor de grabación utiliza el almacenamiento borde de una cámara. Por lo general, los sitios remotos están en línea con su sitio central, alimentándolo una transmisión en vivo que los registros centrales del sitio. En caso de que la red falla por alguna razón, el sitio central se pierde en las secuencias de grabación. Sin embargo, una vez que se restablece la red, el sitio central recupera automáticamente grabaciones remotas que cubren la baja periodo. Esto requiere el uso de la **recuperación automática de grabaciones remotas cuando la conexión se restablece** la opción (ver "Recuperar grabaciones remotas desde un sitio remoto cámara" en la página 312) sobre la pestaña **registro** para la cámara.

Usted puede mezclar cualquiera de las soluciones anteriores para satisfacer sus necesidades especiales de las organizaciones.

Añadir un sitio remoto a su sitio central de Milestone Interconnect

Agrega sitios remotos al sitio central con el Asistente **Añadir hardware**.

Requisitos

- Número suficiente de cámara Milestone Interconnect (ver "Milestone Interconnect y concesión de licencias" en la página 308) licencias.
- Otra configurado y funcionando XProtect, Milestone Husky NVR, o Milestone Arcus sistema que incluye una cuenta de usuario (usuarios básicos, el usuario local de Windows o Windows usuario de Active Directory) con los derechos de los dispositivos que el sistema XProtect Corporate central debe ser capaz de acceder.
- Conexión de red entre el XProtect Corporate site central y los sitios remotos con acceso o reenvío de puertos para los puertos que se utilizan en los sitios remotos.

Para añadir un sitio remoto:

1. En el sitio central, expanda **Servidores** y seleccione **servidores de grabación**.
2. En el panel Descripción general, expanda el servidor de grabación en cuestión y haga clic.
3. Seleccionar **Añadir hardware** para iniciar el asistente.

4. En la primera página seleccione **Escaneo de rangos de direcciones** o **Manual** y haga clic en **Siguiente**.

5. Especificar nombres de usuario y contraseñas. La cuenta de usuario se debe definir previamente en el sistema remoto. Puede añadir nombres de usuario y contraseñas según sea necesario haciendo clic en **Añadir**. Cuando esté listo, haga clic en **Siguiente**.

6. Seleccionar los controladores a utilizar cuando se escanea. En este caso elegir entre los controladores de Milestone. Haga clic en **Siguiente**.

7. Especificar las direcciones IP y números de puerto que desea analizar. El valor predeterminado es el puerto 80. Haga clic en **Siguiente**.

   Espere mientras el sistema detecta los sitios remotos. Un indicador de estado muestra el proceso de detección. En caso de una detección satisfactoria, un mensaje **Correcto** aparece en la columna **Estado**. Si no puede añadir, puede hacer clic en el **Error** mensaje de error para ver por qué.

8. Optar por activar o desactivar los sistemas detectados con éxito. Haga clic en **Siguiente**.

9. Espere mientras el sistema detecta el hardware y recoge la información específica del dispositivo. Haga clic en **Siguiente**.

10. Optar por activar o desactivar los dispositivos de hardware y detectado correctamente. Haga clic en **Siguiente**.

11. Seleccionar un grupo predeterminado. Haga clic en **Finalizar**.

12. Después de la instalación, se puede ver el sistema y sus dispositivos en el panel **general**.

    En función de los derechos de usuario para el usuario seleccionado en el sitio remoto, el sitio central tiene acceso a todas las cámaras y las funciones o un subconjunto de ellos.

Asignar derechos de usuario

Configura derechos de usuario para una cámara interconectada como lo hace con otras cámaras, mediante la creación de un cometido y la asignación de acceso a las funciones.

1. En el sitio central, en el panel **navegación del sitio**, ampliar **Seguridad** y seleccione **Cometidos**.

2. En el panel Descripción general, haga clic en la función de administrador integrada y seleccione **Añadir cometido** (ver "**Añadir y gestionar un cometido**" en la página 230).

3. Nombrar el cometido y configurar los ajustes en la pestaña **dispositivo** (ver "**Pestaña Dispositivo (cometidos)**" en la página 251) y la pestaña **grabaciones remotas** (ver "**Pestaña Grabaciones remoto (cometidos)**" en la página 258).

Actualización de sitio remoto de hardware

Si la configuración ha sido cambiado en un sitio remoto, por ejemplo, añadido o cámaras y eventos quitado, deberá actualizar la configuración en el sitio central para reflejar la nueva configuración en el sitio remoto.

1. En el sitio central, expanda **Servidores** y seleccione **Servidores de grabación.**

2. En el panel Descripción general, expanda el servidor de grabación es necesario, seleccione el sistema remoto relevante. Haga clic derecho en él.

3. Seleccione **Actualización del hardware**. Esto abre el cuadro de diálogo de **actualización de hardware**.

4. Las listas de los cuadros de diálogo de todos los cambios (dispositivos retirados, actualizan y se añaden) en el sistema remoto desde la configuración de Milestone Interconnect se estableció o actualizan pasado. Haga clic en **Confirmar** para actualizar su sitio central con estos cambios.

Establecer la conexión de escritorio remoto para sistema remoto

Puede conectarse de forma remota a sistemas en su configuración Milestone Interconnect.

Requisitos
Las conexiones de escritorio remoto en el equipo que desea remoto para deben estar en funcionamiento.

Esta función no es compatible con el hardware habilitado para Milestone Arcus.

1. En el sitio central, expanda **Servidores** y seleccione **Servidores de grabación.**
2. En el panel Descripción general, expanda el servidor de grabación es necesario, seleccione el sistema remoto relevante.
3. En el panel Propiedades, seleccione la pestaña **Información**.
4. En la **remota área de la administración**, escriba el nombre apropiado de usuario y contraseña de Windows.
5. Una vez que el nombre de usuario y la contraseña se guardan, haga clic en **Conectar** para establecer la conexión de escritorio remoto.
6. En la barra de herramientas, haga clic en **Guardar**.

Habilitar la reproducción directamente desde el sitio remoto de la cámara

Si su sitio central está conectado continuamente con sus sitios remotos, puede configurar el sistema para que los usuarios de reproducción de las grabaciones directamente desde los sitios remotos. Ver también configuraciones Milestone Interconnect posibles (ver "Milestone Interconnect configuraciones (explicado)" en la página 309).

1. En el sitio central, expanda **Servidores** y seleccione **Servidores de grabación.**
2. En el panel Descripción general, expanda el servidor de grabación es necesario, seleccione el sistema remoto relevante. Seleccione la cámara interconectada relevante.
3. En el panel Propiedades, seleccione la pestaña **Registro** y seleccionar la opción **Reproducir las grabaciones desde el sistema remoto**.
4. En la barra de herramientas, haga clic en **Guardar**.

En una configuración Milestone Interconnect, el sitio central ignora las máscaras de privacidad definidas en un sitio remoto. Si desea aplicar las mismas máscaras de privacidad, debe redefinirlas en el sitio central.

Recuperar grabaciones remotas desde un sitio remoto cámara

Si su sitio central **no** es conectado continuamente con sus sitios remotos, puede configurar su sistema para almacenar centralmente grabaciones remotas y puede configurar la recuperación de grabaciones remotas cuando la conexión de red es óptima. Ver también configuraciones Milestone Interconnect posibles (ver "Milestone Interconnect configuraciones (explicado)" en la página 309).

Para permitir a los usuarios recuperar realidad grabaciones, debe habilitar este permiso para que el cometido relevante (ver "Pestaña Grabaciones remoto (cometidos)" en la página 258).

Para configurar el sistema:

1. En el sitio central, expanda **Servidores** y seleccione **Servidores de grabación.**
2. En el panel Descripción general, expanda el servidor de grabación es necesario, seleccione el sistema remoto relevante. Seleccione el servidor remoto relevante.
3. En el panel Propiedades, seleccione la pestaña **Recuperación a distancia** y actualizar los ajustes (ver "Pestaña Recuperación remota" en la página 119).

Si la red falla por alguna razón, el sitio central pierde las secuencias de grabación. Puede configurar su sistema para permitir que el sitio central recupere automáticamente las grabaciones remotas para cubrir el período de espera, una vez que se restablezca la red.

1. En el sitio central, expanda **Servidores** y seleccione **Servidores de grabación.**
2. En el panel Descripción general, expanda el servidor de grabación es necesario, seleccione el sistema remoto relevante. Seleccione la cámara correspondiente.
3. En el panel Propiedades, seleccione la pestaña **Registro** y seleccione la opción **Recupera automáticamente las grabaciones a distancia cuando se restaura la conexión** (ver "**Grabación remota (explicada)**" en la página 141).
4. En la barra de herramientas, haga clic en **Guardar**.

Como alternativa, puede utilizar reglas o iniciar recuperaciones de grabación remota de XProtect Smart Client cuando sea necesario.

En una configuración Milestone Interconnect, el sitio central ignora las máscaras de privacidad definidas en un sitio remoto. Si desea aplicar las mismas máscaras de privacidad, debe redefinirlas en el sitio central.

Configurar su sitio central para responder a eventos desde sitios remotos

Puede usar los eventos definidos en los sitios remotos para activar reglas y alarmas en su sitio central y con ello responder de manera inmediata a los acontecimientos de los sitios remotos. Esto requiere que los sitios remotos están conectados y en línea. El número y tipo de eventos dependen de los eventos configurados y predefinidos en los sitios remotos.

La lista de eventos admitidos está disponible en el Milestone sitio web (http://www.milestonesys.com/our-products/milestone-interconnect/milestone-interconnect-compatibility).

No se puede eliminar eventos predefinidos.

Requisitos:

- Si desea utilizar / eventos manuales definidos por el usuario de los sitios remotos como desencadenante de eventos, primero debe crear estos en los sitios remotos.
- Asegúrese de que usted tiene una lista actualizada de los eventos de los sitios remotos (ver "Actualización de sitio remoto de hardware" en la página 311).

Añadir un evento definido por el usuario / manual desde un sitio remoto

1. En el sitio central, expanda **Servidores** y seleccione **servidores de grabación**.

2. En el panel Descripción general, seleccione el servidor remoto relevante y la **pestaña Eventos**.
3. La lista contiene los eventos predefinidos. Haga clic en **Añadir** para incluir eventos definidos por el usuario o eventos manuales desde el sitio remoto de la lista.

Utilice un evento en un sitio remoto para activar una alarma en el sitio central:

1. En el sitio central, ampliar **Alarmas** y seleccione **Definiciones de alarma**.
2. En el panel Descripción general, haga clic en **Definiciones de alarma** y haga clic en **Añadir nuevo**.
3. Introduzca los valores según sea necesario.
4. En el campo **Evento activador**, puede seleccionar entre los eventos predefinidos y definidos por el usuario soportadas.
5. En el campo **Fuentes**, seleccione el servidor remoto que representa el sitio remoto que desea alarmas de.
6. Guarde la configuración cuando haya terminado.

Utilice un evento en un sitio remoto para desencadenar una acción basada en reglas en el sitio central:

1. En el sitio central, ampliar **Reglas y Eventos** y seleccione **Reglas**.
2. En el panel Descripción general, haga clic en **Reglas** y haga clic en **Añadir regla**.
3. En el asistente que aparece, seleccione **Realizar una acción en <evento>**.
4. En la zona **Editar la descripción de la regla**, haga clic en **evento** y seleccione entre los eventos predefinidos y definidos por el usuario. **Haga clic en OK (aceptar)**.
5. Haga clic en **dispositivos / servidor de grabación / servidor de administración** y seleccione el servidor remoto que representa el sitio remoto que desea que el sitio central inicie una acción. **Haga clic en OK (aceptar)**.
6. Haga clic en **Siguiente** para llegar a la siguiente página del asistente.
7. Seleccione las condiciones que desea aplicar para esta regla. Si no selecciona ninguna condición, la regla se aplica siempre. Haga clic en **Siguiente**.
8. Seleccione una acción y especifique los detalles en la zona **Editar la descripción de la regla**. Haga clic en **Siguiente**.
9. Seleccionar un criterio de parada, si es necesario. Haga clic en **Siguiente**.
10. Seleccione una acción de parada, si es necesario. Haga clic en **Finalizar**.

Plano inteligente

Archivos de plano inteligente en caché (explicado)

Los archivos que utilice para su fondo geográfico se recuperan de un servidor de mosaico. El tiempo que los archivos se almacenan en la carpeta de caché depende del valor seleccionado en la lista **Eliminar los archivos en caché del plano inteligente** en **Opciones** en XProtect Smart Client.Los archivos se almacenan bien:

- Indefinidamente (**nunca**)
- Durante 30 días si el archivo no se utiliza (**cuando no se utiliza durante 30 días**)
- Cuando el operador sale XProtect Smart Client (**en la salida**).

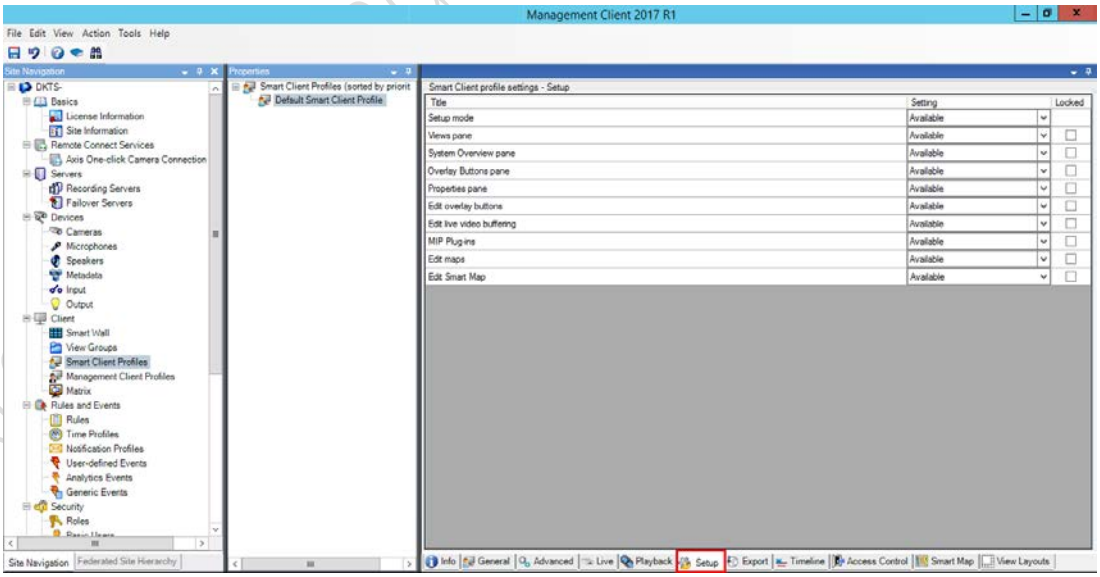
Cuando cambia la dirección del servidor de mosaico, automáticamente se crea una nueva carpeta de caché. Los archivos de mapas anteriores se conservan en la carpeta de caché asociada en su equipo local.

Habilitar la edición de planos inteligentes

Los operadores pueden editar planos inteligentes en XProtect Smart Client en el modo de configuración sólo si la edición está habilitada en Management Client. Si aún no está habilitado, debe habilitar la edición para cada perfil relevante de Smart Client.

Pasos:

1. En el panel **Navegación del sitio**, expanda el nodo **Cliente**.
2. Haga clic en **Perfiles Smart Client**.



3. En el panel general, seleccione el perfil Smart Client relevante.
4. En el panel **Propiedades**, haga clic en la ficha **Configuración**.
5. En el **Editar plano inteligente** lista, seleccione **Disponible**.
6. Repita estos pasos para cada perfil relevante de Smart Client.

7. Guarde los cambios. La próxima vez que los usuarios asignados al perfil Smart Client que haya seleccionado inicien en XProtect Smart Client, podrán editar planos inteligentes.

Para desactivar la edición, en **Editar plano inteligente** lista, seleccione **No disponible**.

Habilitar la edición de cámaras en plano inteligente

Para permitir que los operadores posicionen una cámara en el plano inteligente, ajuste el campo de visión y la dirección, debe habilitar la edición de cámaras por cometido.

Requisitos
Antes de empezar, asegúrese de que Se ha habilitado la edición de planos inteligente (ver "Habilitar la edición de planos inteligentes" en la página 315). Haga esto en el perfil Smart Client al que está asociada el cometido del operador.

Pasos:

1. Expanda el nodo **seguridad**> **Cometidos**.
2. En el panel **Cometidos**, seleccione el cometido a la que está asociado su operador.
3. Para dar los derechos de edición de cometido:
   - Haga clic en la pestaña **Seguridad general** y seleccione **Cámaras** en el panel de **Configuración de cometido**.
   - En la columna **Permitir** , seleccione el **Control total** o **Casilla de verificación Editar** .
4. Guardar los cambios.

Los pasos anteriores le dan al cometido el derecho de editar todas las cámaras.Para habilitar la edición de cámaras individuales, vaya a la ficha **Dispositivo** y seleccione la cámara correspondiente.

Configuración de fondos geográficos

El mapa del mundo básico es el fondo geográfico predeterminado, y no requiere ninguna configuración. También puede utilizar OpenStreetMaps fuera de la caja sin pasos adicionales si su sistema puede acceder a Internet. Para obtener información sobre los otros tipos de fondos, consulte Tipos de fondos geográficos (ver "Tipos de entornos geográficos (explicación)" en la página 317).

Requisitos para usar Bing Maps y Google Maps:

1. El administrador del sistema debe ingresar la clave Bing Maps o la clave criptográfica privada y el ID de cliente de Google Maps en Management Client para un perfil Smart Client. Los fondos geográficos de Bing Maps y Google Maps sólo están disponibles en XProtect Smart Client después de que el administrador lo haga.
2. Utilice su cuenta de Google Maps o Bing Maps para crear o comprar una clave para Bing Maps, o un ID de cliente y una clave privada para la API de Google Maps. Para obtener más información, consulte Seleccionar plan para las API de Google Maps y Bing Maps (ver "Seleccione un plan para las API de Google Maps o Bing Maps" en la página 307).

Si desea evitar que los usuarios utilicen OpenStreetMaps como fondo geográfico, haga clic en **Configuración**, y seleccione **Indisponible** para el **Fondo geográfico de OpenStreetMap** opción. Entonces XProtect Smart Client no lo muestra como una opción para un plano inteligente.

Tipos de entornos geográficos (explicación)

Después de añadir un Plano Inteligente a una vista, puede elegir uno de los siguientes entornos geográficos:

- **Mapamundi básico**: usa el entorno geográfico estándar proporcionado en XProtect Smart Client. Este plano está diseñado para usar como referencia general, y no posee funciones como límites de países, ciudades u otros detalles. Sin embargo, como los otros entornos geográficos, no posee datos de geo-referencia.
- **Bing Maps**: conectado a Bing Maps.
- **Google Maps**: conectado a Google Maps.

  Nota: Las opciones de Bing Maps y Google Maps requieren acceso a Internet, y debe adquirir una clave de Microsoft o Google.

- **OpenStreetMap**: conecta con el proyecto de mapeo de código abierto OpenStreetMap (http://www.openstreetmap.org) (OSM). Esta opción precisa acceso a Internet. Los datos de plano para OSM se proporcionan en la Licencia de base de datos abierta (www.openstreetmap.org/copyright).
- **Nada**: esta opción oculta el entorno geográfico. Sin embargo, los datos de geo-referencia siguen ahí. Para más información, consulte Trabajar con capas en un Plano Inteligente.

De manera predeterminada, Bing Maps y Google Maps muestran imágenes del satélite. Puede cambiar las imágenes, por ejemplo de aéreas a de terreno, para ver los diferentes detalles. Para obtener más información, consulte Cambiar el entorno geográfico a un Plano Inteligente.

Ingrese la clave de Bing Maps o la clave de Google Maps o el ID de cliente en Management Client

Puede poner una clave a disposición de varios usuarios escribiéndola para un perfil Smart Client en Management Client. Todos los usuarios asignados al perfil utilizarán esta clave.

Si desea utilizar una clave diferente, puede introducirla en el cuadro de diálogo **Opciones** en Smart Client. Esto requiere que el administrador del sistema no haya bloqueado la clave en Management Client y que la casilla de verificación **Seguir servidor** no esté seleccionada en Smart Client. La clave de Smart Client está asociada con su cuenta de usuario, y sólo usted la utilizará.

Pasos:

1. En Management Client, en el panel **Site Navigation** , haga clic en **Smart Client perfiles**.
2. En el panel **Propiedades**, seleccione el perfil Smart Client y, a continuación, haga clic en la ficha **Plano inteligente**.
   - Para Bing Maps, ingrese la clave en el campo **Bing Maps** .
   - Para Google Maps, ingrese la información que recibió para su Plan Premium en el **ID de cliente de Google Maps** y **Clave privada para los campos de Google Maps** .
3. A continuación, ingresa la clave de Bing Maps o la clave privada y el ID de cliente de Google Maps en XProtect Smart Client (ver "Ingrese la clave de Bing Maps o la clave privada y el ID de cliente de Google Maps en XProtect Smart Client" en la página 317).

Ingrese la clave de Bing Maps o la clave privada y el ID de cliente de Google Maps en XProtect Smart Client

Si desea utilizar una clave diferente y no utilizar la clave del perfil Smart Client al que está asignado, puede introducir la clave en XProtect Smart Client. Si introduce una clave en XProtect Smart Client, se asociará con su cuenta de usuario y solo la utilizará.

Pasos:

1. En la esquina superior derecha del área de trabajo, haga clic en **Configuración**.
2. En la ventana **Configuración** , en el panel de navegación, haga clic en **Plano inteligente**.
3. Dependiendo del servicio de mapas que desee utilizar, realice una de las siguientes acciones:
   - Para Bing Maps, ingrese la clave en el campo **Bing Maps** .
   - Para Google Maps, ingrese la información que recibió para su Plan Premium en el **ID de cliente de Google Maps** y **Clave privada para los campos de Google Maps** .

Cambio del servidor de archivos de OpenStreetMap

Si utiliza OpenStreetMap como contexto geográfico para su plano inteligente, puede cambiar la ubicación desde donde se obtienen las imágenes guardadas en el servidor. Las imágenes de mosaico son las que componen el mapa. Para hecho debe cambiar la dirección del servidor de archivos. Así podrá utilizar el servidor de archivos local, por ejemplo, si su organización tiene sus propios mapas para zonas como aeropuertos y puertos. Utilizar un servidor local permite queXProtect Smart Clientpueda recuperar imágenes de planos sin acceso a Internet.

También puede usar un servidor de archivos comercial. Milestone no ofrece ninguna solución de servidor de archivos para OpenStreetMap.

La dirección del servidor de archivos se puede especificar de dos maneras:

- En Management Client - Escriba la dirección del servidor de archivos en los perfiles Smart Client (ver "Establecer un servidor de mosaico OpenStreetMap alternativo" en la página 318). La dirección del servidor se aplica a todos los usuarios de Smart Client asignados a los perfiles individuales de Smart Client.
- En XProtect Smart Client: escriba la dirección del servidor de archivos en el cuadro de diálogo **Ajustes**. La dirección del servidor se aplica solo a esa instalación de Smart Client.

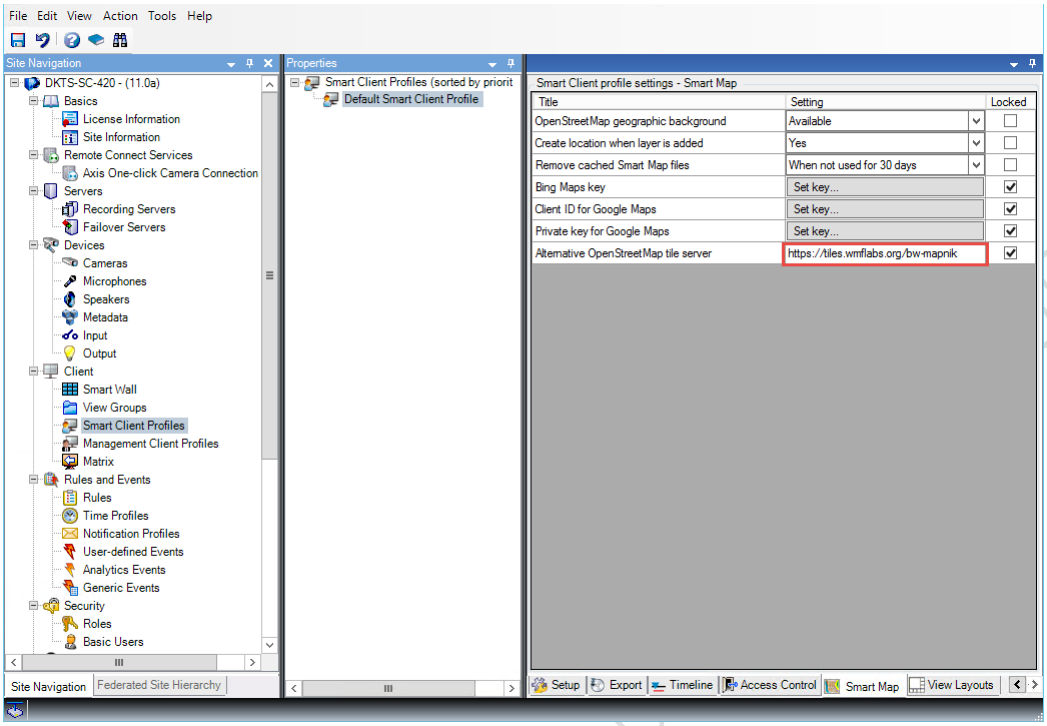
Establecer un servidor de mosaico OpenStreetMap alternativo

Para la función de plano inteligente, puede especificar un servidor de mosaico OpenStreetMap alternativo, donde el VMS recupera los archivos de mapa para el fondo geográfico. El servidor que especifique está asociado con un perfil Smart Client, de modo que los usuarios asignados al perfil Smart Client vean el mismo OpenStreetMap en XProtect Smart Client.

Pasos:

1. En el panel **Navegación del sitio**, expanda el nodo **Cliente** y haga clic en **Perfiles Smart Client**.

2. En el panel general, seleccione el perfil Smart Client relevante.



3. En el panel Propiedades, haga clic en la ficha **Plano inteligente**.

4. En el campo **Alternativa de servidor de mosaico OpenStreetMap**, ingrese la dirección del servidor de mosaico.

5. Si desea evitar que los usuarios XProtect Smart Client cambien la configuración, seleccione la casilla **Bloqueada**.

6. Guardar los cambios.

Establecer la posición de la cámara, la dirección, el campo de visión y la profundidad (plano inteligente)

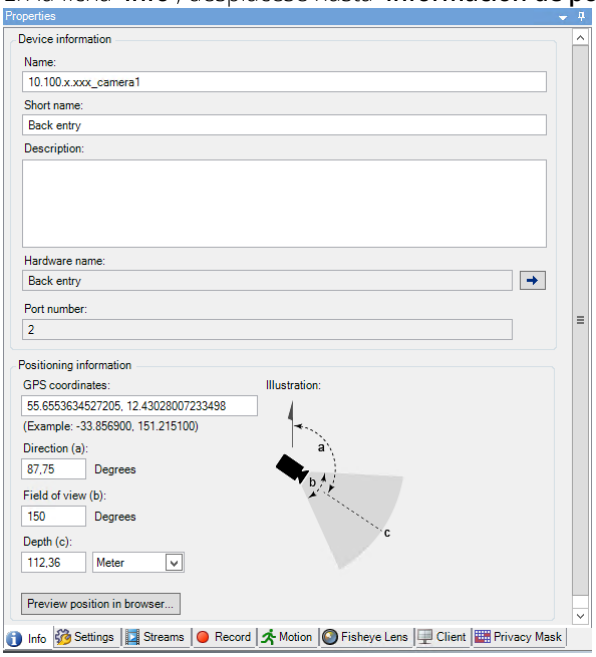
Para asegurarse de que la cámara está colocada correctamente en el plano inteligente, puede configurar las coordenadas GPS, la dirección de la cámara, el campo de visión y la profundidad de visualización. Al hacerlo, automáticamente la cámara se agrega al plano inteligente la próxima vez que un operador lo cargue en XProtect Smart Client.

Pasos:

1. En Management Client, expanda el nodo **Dispositivos** y seleccione **Cámaras**.

2. En el panel **Dispositivos** , seleccione el grupo de cámara y la cámara correspondientes.

3. En la ficha **Info** , desplácese hasta **Información de posicionamiento** .



4. Especifique la latitud y la longitud en el **coordenadas GPS** de campo, en ese orden.Utilice un punto como separador decimal y una coma para separar los valores.

5. En el campo **Dirección** , ingrese un valor en el rango de 0 y 360 grados.

6. En el campo **Campo de visión** , ingrese un valor en el rango de 0 y 360 grados.

7. En el campo **Profundidad** , ingrese la profundidad de visualización, ya sea en metros o pies.

8. Guardar los cambios.

También puede configurar las propiedades en los servidores de grabación.

Configurando un plano inteligente con Milestone Federated Architecture

Cuando utiliza el plano inteligente en un Milestone Federated Architecture, todas las cámaras de los sitios conectados aparecen en el plano inteligente. Los pasos generales en este tema describen cómo configurar el plano inteligente en una arquitectura federada.

Para obtener información general sobre Milestone Federated Architecture, consulte Milestone Federated Architecture (explicado) (en la página 298).

1. Antes de conectar el sitio principal con los subsitios, asegúrese de que se hayan especificado las coordenadas GPS en todas las cámaras en todos los sitios. Las coordenadas de GPS se agregan automáticamente cuando una cámara se coloca en el plano inteligente a través de XProtect Smart Client, pero también puede agregarlas manualmente en Management Client en las propiedades de la cámara. Para obtener más información, consulte Establezca la posición, dirección, campo de visión y profundidad de la cámara (ver "Establecer la posición de la cámara, la dirección, el campo de visión y la profundidad (plano inteligente)" en la página 319).

2. Debe agregar los operadores Smart Client como usuarios de Windows en el sitio principal y todos los subsitios. Al menos en el sitio principal, los usuarios de Windows deben tener derechos de edición de

planos inteligentes. Esto les permite editar el plano inteligente para el sitio principal y todos los subsitios. A continuación, debe determinar si los usuarios de Windows en los subsitios necesitan derechos de edición de planos inteligentes. En Management Client, primero crea los usuarios de Windows bajo **Cometidos**, y luego habilita la edición de planos mapa inteligentes. Para obtener más información, consulte Habilite la edición de planos inteligentes (ver "Habilitar la edición de planos inteligentes" en la página 315).

3. En el sitio principal, debe agregar los subsitios como usuarios de Windows a un rol con derechos de administrador. Cuando especifica el tipo de objeto, seleccione la casilla de verificación **Computadoras**.

4. En cada uno de los subsitios, debe agregar el sitio primario como usuario de Windows al mismo rol de administrador que se usa en el sitio primario. Cuando especifica el tipo de objeto, seleccione la casilla de verificación **Computadoras**.

5. En el sitio primario, asegúrese de que puede ver la ventana **Jerarquía de sitios federados**. En Management Client, vaya a **Vista** y seleccione **Jerarquía de sitios federados**. Agregue cada uno de los subsitios al sitio principal. Para obtener más información, consulte Agregar sitio a la jerarquía (ver "Añadir sitio a la jerarquía" en la página 303).

6. Ahora puedes probar que funciona en XProtect Smart Client. Inicie sesión en el sitio principal como administrador o como operador, y abra una vista que contenga el plano inteligente. Si la configuración se ha realizado correctamente, todas las cámaras tanto del sitio principal como de todos los subsitios aparecerán en el plano inteligente. Si inicia sesión en uno de los subsitios, verá solo las cámaras de ese sitio y sus subsitios.

Para editar cámaras en un plano inteligente, por ejemplo, la posición y el ángulo de la cámara, los usuarios necesitan derechos de edición de la cámara.

Solución de problemas (plano inteligente)

Error al agregar la cámara al plano inteligente

Error

Si un operador intenta agregar cámaras a un plano inteligente manualmente, porque las cámaras no se agregaron automáticamente al cargar el plano inteligente, puede aparecer el siguiente error: No se puede guardar el plano. No se puede realizar la operación.

Lo que puede causar el error es que el operador está ejecutando la versión 2017 R1 de XProtect Smart Client contra una instalación XProtect Corporate 2017 R2.XProtect Smart Client busca la posición GPS de la cámara en el servidor de eventos, pero en la versión 2017 R2 o más reciente de XProtect Corporate, la posición GPS se almacena en el servidor de administración.

Solución

Actualice XProtect Smart Client a la versión 2017 R2 o posterior.

XProtect Smart Wall

XProtect Smart Wall (explicado)

Funcionalidad disponible depende del sistema que está utilizando. Ver tabla de comparación de productos (en la página 24) para más información.

XProtect Smart Wall es un producto de pared de video avanzado que proporciona conocimiento de la situación supremo en centros de vigilancia más grandes y ayuda a los operadores de vigilancia para centrarse en lo que es importante garantizar una mayor eficiencia y tiempos de respuesta más cortos.

XProtect Smart Wall permite el cambio rápido de vídeo en directo que aparece en la pantalla de vídeo para satisfacer las necesidades de seguridad y escenarios específicos. Una manera de cambiar lo que se visualiza en la pantalla de vídeo es con los valores preestablecidos de Smart Wall. El administrador de vigilancia define los valores preestablecidos de Smart Wall en Management Client para optimizar la cobertura de vigilancia para diferentes escenarios de vigilancia recurrentes. Valores preestablecidos de Smart Wall trabajan por toda la pared de vídeo o partes de la pantalla de vídeo y determinar el que se muestran las cámaras y la distribución de los contenidos en los monitores en la pantalla de vídeo.

Con los valores preestablecidos de Smart Wall, la pantalla cambia pueden activarse automáticamente mediante reglas. La pantalla cambia también se pueden activar manualmente por los operadores de vigilancia utilizando XProtect Smart Client arrastrando y soltando vistas y cámaras en la representación lógica de la pantalla de vídeo en el XProtect Smart Client o mediante la selección de los diferentes valores preestablecidos de Smart Wall que define el administrador de vigilancia.

Consulte la documentación de XProtect Smart Client para obtener más información acerca de cómo utilizar las características de XProtect Smart Wall en XProtect Smart Client.

Licencias XProtect Smart Wall

XProtect Smart Wall requiere de las siguientes licencias relacionadas con la pared de vídeo:

- Una **licencia base** para XProtect Smart Wall que cubre un número ilimitado de monitores que muestran vídeo en una pared de vídeo.

Una licencia base para XProtect Smart Wall se incluye en la licencia de base para XProtect Corporate. Si tiene XProtect Expert, puede adquirir una licencia base para XProtect Smart Wall por separado.

Configurar Smart Walls

Una configuración de Smart Wall consiste en definir el Smart Wall, añadiendo monitores y definir el diseño del monitor, y opcionalmente especificar valores preestablecidos de Smart Wall y el diseño y el contenido de los diferentes monitores.

No es necesario definir valores preestablecidos de Smart Wall, si sólo desea visualizar cámaras y XProtect Smart Client puntos de vista que sus usuarios XProtect Smart Client de forma manual puede empujar a la pantalla de vídeo.

Si desea utilizar reglas para cambiar automáticamente lo que se muestra en la pared de vídeo, o si tiene escenarios de vigilancia típicos en los que desea mostrar el mismo contenido en la pared de vídeo cada vez que ocurre el escenario, debe definir preajustes Smart Wall.

La configuración de la Smart Wall es muy flexible. Puede incluir todos los monitores en la pantalla de vídeo en una Smart Wall o un grupo los monitores y configurar un Smart Wall para cada grupo. Preajustes Smart Wall se puede cambiar el diseño y el contenido de todos los monitores en una Smart Wall o solamente algunos de los monitores. Los monitores pueden ser parte de varias Smart Wall y valores preestablecidos de Smart Wall. Crear tantas Smart Wall y valores preestablecidos de Smart Wall que necesita para optimizar la cobertura de sus escenarios típicos de vigilancia.

a. Definir el Smart Wall

1. Expanda **Cliente**, y seleccione **Smart Wall**.
2. En el panel **general**, haga clic **Smart Walls** y seleccione **Añadir Smart Wall**.
3. Especificar la configuración de la Smart Wall.
4. En la configuración **Propiedades de elemento de vista general** , defina si desea que la información de estado del sistema y las barras de título aparezcan encima de los elementos de diseño de las cámaras.
5. Haga clic en **OK** (aceptar).

b. Añadir monitores y definir el diseño del monitor

1. Haga clic con el Smart Wall y seleccione **Añadir monitor**.
2. Configurar las dimensiones del monitor de forma que se asemeja a uno de los monitores físicos en la pantalla de vídeo.
3. Utilice los ajustes de comportamiento preestablecidos **Valor preestablecido vacío** y **Elemento de valor preestablecido vacío** para definir lo que se muestra en un monitor con una disposición preestablecida vacía o en los elementos predeterminados vacíos cuando un nuevo preset Smart Wall se activa automáticamente o se selecciona manualmente en XProtect Smart Client. Puede usar los preajustes de vacíos y puntos de Programación vacío de contenido no está controlado por el valor preestablecido de Smart Wall.
4. Utilice el ajuste de comportamiento preestablecido **Inserción de elemento** para definir lo que debe suceder cuando un usuario de XProtect Smart Client arrastra una cámara en un elemento de diseño en el preset Smart Wall. Seleccionar **Independiente** para reemplazar la cámara ya en el elemento preestablecido con la nueva cámara o **Vinculado** para empujar el contenido de los elementos de diseño de izquierda a derecha, desde donde se insertó la nueva cámara.
5. Añadir tantos monitores como usted tiene en la pared de vídeo física.

6. Seleccione el Smart Wall y en la pestaña **Disposición**, haga clic en **Editar** para posicionar los diferentes monitores para que sus posiciones se parecen al montaje de los monitores físicos en la pantalla de vídeo.

7. Haga clic en **OK**. La misma disposición se utiliza en XProtect Smart Client.

c. Añadir valores preestablecidos de Smart Wall (opcional)

1. Seleccione el Smart Wall y pestaña de los **ajustes preestablecidos**, haga clic en **Añadir nuevo**.

2. Introduzca un nombre y una descripción y haga clic en **OK**.

3. Haga clic en **Activar** para mostrar el valor preestablecido de Smart Wall en la pantalla de vídeo.

4. Crear tantos valores preestablecidos de Smart Wall como sea necesario.

d. Añadir el diseño y las cámaras a los monitores (requiere un valor preestablecido Smart Wall)

1. Seleccione uno de los monitores que creó y, en la ficha **Posiciones preestablecidas**, seleccione un preset de la lista para configurar lo que desea que muestre el monitor seleccionado cuando se utilice con el preset Smart Wall seleccionado.

2. Haga clic en **Editar**.

3. Haga clic en el botón Diseño para seleccionar qué diseño para utilizar con el monitor y haga clic en **OK**.


4. Arrastre las cámaras de los **grupos de dispositivos**, **Servidores de grabación** o **Jerarquía de sitios federados** ficha en los elementos de diseño diferentes. Las cámaras de la pestaña **Jerarquía de sitios federados** están accesibles en una configuración Milestone Federated Architecture. Puede dejar los elementos de diseño en blanco, para que estén disponibles para otros contenidos que no esté controlado por el valor preestablecido de Smart Wall.

5. Si el monitor ya tiene un diseño para el preset seleccionado, puede hacer clic en **Limpiar** para definir un nuevo diseño o excluir el monitor del preset Smart Wall, por lo que el monitor está disponible para otro contenido no controlado por el Smart Wall programar.

6. **Haga clic en OK (aceptar)**.

7. Repita los pasos, hasta que haya agregado un diseño y cámaras en los monitores que desee incluir en el valor preestablecido Smart Wall.

Configurar los derechos sobre el XProtect Smart Wall

Puede controlar las tareas que los usuarios XProtect Smart Client pueden realizar en XProtect Smart Wall mediante la especificación de derechos de usuario para los cometidos. Los derechos de usuario se aplican a todos los usuarios que están asignados a la función. Para obtener más información, consulte Cometidos con la Smart Wall propiedades (ver "Pestaña Smart Wall (cometidos)" en la página 258) derechos.

Selecciones para el **Leer**, **Editar** y **Eliminar** se aplican siempre los derechos de usuario. Para los derechos de usuario **Operar** y **Reproducción**, también puede conceder los derechos de usuario durante un período de tiempo específico seleccionando un perfil temporal. Por ejemplo, esto es útil si desea permitir a un usuario cambiar el contenido que se muestra en una Smart Wall, pero sólo durante las horas normales de trabajo.

Para especificar derechos de usuario para un cometido, siga estos pasos:

1. En el panel de navegación del sitio, expanda **Seguridad**, y seleccione **Cometidos**.
2. En el panel **Cometidos**, seleccione el cometido, o crear un nuevo cometido haciendo clic derecho en el panel y seleccionando **Añadir cometido**.
3. En la parte superior de panel **Configuración de cometido**, seleccione el Smart Wall.
4. En la parte inferior del panel de Configuración de cometido, haga clic en la pestaña **Smart Wall** y, a continuación, seleccione los derechos de usuario para asignar.
   - **Leer** - ver Smart Wall en aplicaciones cliente
   - **Editar** - Modificar Smart Walls en aplicaciones cliente
   - **Eliminar** - Eliminar Smart Walls en aplicaciones cliente
   - **Operar** - Aplicar diseños en el monitor seleccionado en aplicaciones cliente, y activar ajustes preestablecidos
   - **Reproducción** - Revisión y gestión de vídeo en directo y grabado

   Nota: Si no selecciona el permiso **Reproducción**, los usuarios pueden ver pero no cambiar el contenido que se muestra en la pared de vídeo. Si un usuario realiza un cambio, el sistema se desconecta automáticamente del estado compartido y el contenido de la pantalla de vídeo no se ve afectada. Para volver a la vista compartida, haga clic en **Volver a conectar Smart Wall monitor**.
5. Opcional: Para conceder derechos **Operar** o **Reproducción** de usuario para un período específico de tiempo, seleccione la casilla de verificación y, a continuación, seleccione el perfil temporal.

Uso de reglas con presets Smart Wall (explicado)

Mediante la combinación de reglas y valores preestablecidos de Smart Wall, se puede controlar lo que aparece en su pantalla de vídeo en forma similar a como el sistema utiliza reglas para controlar el comportamiento de las cámaras y más. Por ejemplo, una regla puede provocar que su pantalla de vídeo para mostrar un cierto valor preestablecido Smart Wall durante un día determinado. Incluso puede utilizar reglas para controlar lo que los monitores individuales en un mural de vídeo. Ver Añadir una regla (en la página 208) para obtener información acerca de cómo crear reglas.

Ejemplo de una regla que provocó un valor preestablecido de Smart Wall:

Propiedades Smart Wall

Pestaña de información (propiedades de la Smart Wall)

En la pestaña **información** para un Smart Wall, se puede añadir y editar Smart Walls.

Nombre	Descripción
Nombre	El nombre de la Smart Wall. Se muestra en el XProtect Smart Client como el nombre del grupo de vista Smart Wall.

Nombre	Descripción
Descripción	Una descripción de la Smart Wall. La descripción sólo se utiliza internamente en el Management Client.
Texto de estado	Si se selecciona, la cámara y el estado del sistema de información se muestra a través de elementos de diseño de cámaras 'en la pantalla de vídeo.
Sin barra de título	Si se selecciona, todos los elementos de diseño Smart Wall no tienen barras de título en la pantalla de vídeo.
Barra de título	Si se selecciona, todos los elementos de diseño Smart Wall tienen barras de título en la pantalla de vídeo.
Barra de título con indicador de directo	Cuando se selecciona, todas las barras de título de elementos de diseño de la Smart Wall muestran indicadores en vivo y en movimiento en la pantalla de vídeo.

Pestaña Preajustes (propiedades de Smart Wall)

En la pestaña **Posiciones preestablecidas** para un Smart Wall, se puede añadir y editar valores preestablecidos de Smart Wall.

Nombre	Descripción
Añadir nuevo	Haga clic para añadir un preset a su instalación de XProtect Smart Wall. Definir un nombre y una descripción para el nuevo valor preestablecido de Smart Wall.
Editar	Editar el nombre y / o descripción de un valor preestablecido de Smart Wall.
Borrar	Eliminar un valor preestablecido Smart Wall.
Activar	Haga clic para mostrar el valor preestablecido de Smart Wall en la pantalla de vídeo. Debe crear reglas con el valor preestablecido de Smart Wall antes de que el sistema puede activar automáticamente la visualización del valor preestablecido de Smart Wall. Consulte también Uso de reglas con presets Smart Wall (explicados) (ver "Uso de reglas con presets Smart Wall (explicado)" en la página 325).

Pestaña de presentación (propiedades de Smart Wall)

En la pestaña **Disposición** para un Smart Wall, coloca los monitores en su Smart Wall para que sus posiciones se parezcan al montaje de los monitores físicos en la pared de vídeo. La disposición también se utiliza en el XProtect Smart Client.

Nombre	Descripción
Editar	Haga clic para ajustar la posición de los monitores.

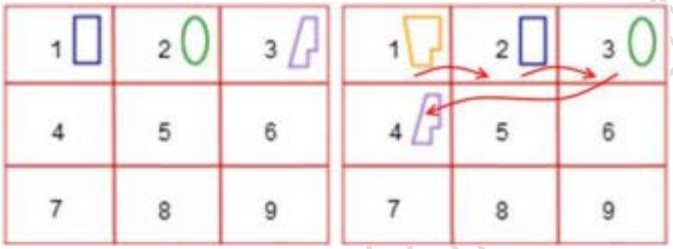
Nombre	Descripción
Movimiento	Para mover un monitor a una nueva posición, seleccione el monitor correspondiente y arrastrarlo hasta la posición deseada, o haga clic en uno de los botones de flecha para mover el monitor en la dirección seleccionada.
Botones de zoom	Haga clic en los botones de zoom acercar / alejar de la disposición de previsualización Smart Wall para asegurar que la posición de los monitores correctamente.
Nombre	El nombre del monitor. El nombre se muestra en el XProtect Smart Client.
Tamaño	El tamaño de la pantalla física en la pantalla de vídeo.
Relación de aspecto	Relación altura/anchura del monitor físico en la pantalla de vídeo.

Propiedades del monitor

Pestaña de información (propiedades del monitor)

En la pestaña **Información** para un monitor en un valor preestablecido de Smart Wall, se puede añadir monitores y editar la configuración de los monitores.

Nombre	Descripción
Nombre	El nombre del monitor. El nombre se muestra en el XProtect Smart Client.
Descripción	Una descripción del monitor. La descripción sólo se utiliza internamente en el Management Client.
Tamaño	El tamaño de la pantalla física en la pantalla de vídeo.
Relación de aspecto	Relación altura/anchura del monitor físico en la pantalla de vídeo.
Valor preestablecido vacío	Define lo que se debe mostrar en un monitor con un diseño preestablecido vacío cuando un nuevo valor preestablecido de Smart Wall se active o se selecciona de XProtect Smart Client. Seleccione **Preservar** para mantener el contenido actual en el monitor. Seleccionar **Borrar** para borrar todo el contenido de modo que nada se visualiza en el monitor.
Elemento de valor preestablecido vacío	Define lo que debe ser representada en un elemento de composición preestablecida vacío cuando un nuevo valor preestablecido de Smart Wall se active o se selecciona de XProtect Smart Client. Seleccione **Preservar** para mantener el contenido actual en el elemento de diseño. Seleccionar **Borrar** para borrar el contenido de modo que nada se muestra en el elemento de diseño.

Nombre	Descripción
Inserción de elemento	Define cómo se insertan las cámaras en el diseño del monitor cuando se ve en el XProtect Smart Client. Al seleccionar **independiente**, sólo cambia el contenido del elemento de diseño afectado, el resto del contenido del diseño sigue siendo el mismo. Al seleccionar **Vinculado**, el contenido de los elementos de diseño se empuja de izquierda a derecha. Si, por ejemplo, una cámara se inserta en la posición 1, la cámara anterior de la posición 1 es empujado a la posición 2, la cámara anterior de la posición 2 es empujado a la posición 3, y así sucesivamente como se ilustra en este ejemplo. 

Pestaña Definiciones (propiedades del monitor)

En la pestaña **ajustes preestablecidos** para un monitor en un valor preestablecido de Smart Wall, se puede editar el diseño y el contenido de la pantalla en el valor preestablecido de Smart Wall seleccionado.

Nombre	Descripción
Preset	Una lista de valores preestablecidos de Smart Wall para el Smart Wall selecto.
Editar	Haga clic en **Editar** para editar el diseño y el contenido de la pantalla seleccionada. Haga doble clic en una cámara para quitar una sola cámara. Haga clic en **Limpiar** para definir un nuevo diseño o excluir el monitor en el valor preestablecido de Smart Wall por lo que el monitor está disponible para otro tipo de contenido que no esté controlado por el valor preestablecido de Smart Wall. Hacer clic  para seleccionar el diseño que desea utilizar con el monitor en el preset seleccionado y haga clic en **OK**. Arrastre las cámaras de los **grupos de dispositivos**, **servidores de grabación** o **Sitios federados** ficha en los elementos de diseño diferentes. Puede dejar objetos de composición vacía, por lo que está disponible para otro tipo de contenido que no esté controlado por el valor preestablecido de Smart Wall.

XProtect Access

Integración de control de acceso (explicado)

El uso de XProtect Access requiere que haya adquirido una licencia base que le permita acceder a esta función en su sistema XProtect. También necesita una licencia de control del acceso a puertas para cada puerta que quiera monitorizar.

Puede utilizar XProtect Access con sistemas de control de acceso de proveedores donde ya exista un plug-in específico para XProtect Access.

La función de integración de control de acceso introduce una nueva funcionalidad que facilita la integración de los sistemas de control de acceso de los clientes con XProtect. Usted obtiene:

- Una interfaz común de usuario operador para múltiples sistemas de control de acceso en XProtect Smart Client.
- Una integración más rápida y más potente de los sistemas de control de acceso.
- Más funcionalidad para el operador (véase más adelante).

En XProtect Smart Client, el operador obtiene:

- Monitoreo en vivo de los eventos en los puntos de acceso.
- Operador pasaje asistido para solicitudes de acceso.
- Integración de mapas.
- Las definiciones de alarma para los eventos de control de acceso.
- Investigación de los eventos en los puntos de acceso.
- Vista general centralizada y control de los estados de la puerta.
- La información y la gestión de los titulares de tarjetas.

El **registro de auditoría** registra los comandos que cada usuario realiza en el sistema de control de acceso de XProtect Smart Client.

Aparte de una licencia base XProtect Access, necesita un plug-in de integración específico del proveedor instalado en el servidor de eventos antes de que pueda iniciar una integración (ver "Configurar un sistema de control de acceso integrado" en la página 330).

Licencias XProtect Access

XProtect Access requiere las siguientes licencias relacionadas con el control de acceso:

- Una **licencia base** para XProtect Access que cubre un número sin restricciones de servidores de acceso.

- Una **licencia de puerta de control de acceso** por puerta que desea integrar y controlar en XProtect Access. **Dos** licencias de puerta de control de acceso se incluyen con la licencia base XProtect Access. Todas las licencias de puertas se instalan automáticamente al instalar el producto XProtect Access. Sin embargo, las licencias de puertas instaladas son desactivada de forma predeterminada que significa que se debe habilitar las puertas que desea utilizar. Sólo se puede activar tantas puertas como licencias tenga las puertas para.

Ejemplo: Usted tiene cinco licencias de puertas de control de acceso y de haber añadido 10 puertas. Una vez que haya añadido cinco puertas, no se puede seleccionar más. Debe eliminar algunos de sus puertas antes de poder añadir otra puerta.

Para encontrar información sobre el estado actual de las licencias de la puerta de control de acceso, expanda el nodo de **control de acceso**.

Para comprar licencias base o licencias de base XProtect Access adicionales, póngase en contacto con su proveedor.

Configurar un sistema de control de acceso integrado

Esta sección proporciona los pasos para una exitosa creación y configuración de un sistema de control de acceso integrado.

Requisitos

- Ha adquirido las licencias XProtect Access necesarias.
- Ha instalado el plug-in de integración específico para su sistema de control de acceso en el servidor de eventos.

1. Añadir el sistema de control de acceso integrado a su sistema XProtect. Ver Asistente para la integración de sistemas de control de acceso (en la página 331). El asistente le lleva a través de los pasos más básicos.
2. Especificar propiedades adicionales para la integración de sistemas de control de acceso, especialmente los eventos de control de acceso pueden requerir que asigne los eventos del sistema de control de acceso con las categorías de eventos que XProtect reconoce. Ver propiedades de control de acceso (en la página 332).
3. Es necesario crear un cometido con el permiso para utilizar las funciones de control de acceso en el XProtect Smart Client. Ver Pestaña Control de acceso (ver "Pestaña Control de acceso (cometidos)" en la página 260).
4. También es necesario asociar este cometido con un perfil de Smart Client. Ver propiedades de perfil de Smart Client (en la página 178).
5. El sistema proporciona una regla predeterminada que le permite acceder a notificaciones de solicitud aparecen en la pantalla XProtect Smart Client en caso de acceso denegado. Puede añadir y modificar las notificaciones de solicitud de acceso, vea Notificación de solicitud de acceso (propriedades) (ver "Pestaña de notificación de solicitud de acceso (Control de acceso)" en la página 334).
6. Puede crear reglas adicionales basados en acciones y eventos del sistema de control de acceso. Ver Acciones y acciones de parada (explicadas) (ver "Acciones y acciones de detención (explicadas)" en la página 185) y Resumen de eventos (ver "Visión general Eventos" en la página 194).
7. Si es necesario, cambie la configuración general de control de acceso en **Opciones** > **Configuración de control de acceso**. Ver Pestaña Configuración de control de acceso (ver "Pestaña Configuración de control de acceso (opciones)" en la página 289).

Asistente para la integración de sistemas de control de acceso

El asistente de **integración de control de acceso** es para la configuración paso a paso de la integración inicial con un sistema de control de acceso. Utilice el asistente para obtener a través de la mayoría de las tareas básicas de configuración. Puede realizar una configuración más detallada posteriormente.

Antes de iniciar el asistente de integración de control de acceso asegurarse de que tiene la integración plug-in instalado en el servidor de eventos.

Algunos de los campos a rellenar y sus valores por defecto se heredan de la integración de plug-in. Por lo tanto, la aparición del asistente puede variar en función del sistema de control de acceso a integrar con.

Para iniciar el asistente, seleccione **control de acceso** en el árbol de nodos, haga clic en y haga clic en **Crear nueva**.

Crear la integración de sistemas de control de acceso

Introduzca el nombre y especificar los detalles de la conexión para el sistema de control de acceso que desea añadir. Los parámetros que deben especificarse dependen del tipo de sistema, pero son típicamente la dirección de red del servidor del sistema de control de acceso y un nombre de usuario y contraseña de administrador de control de acceso.

El sistema de gestión de vídeo utiliza el nombre de usuario y la contraseña especificados para iniciar sesión en el sistema de control de acceso para recuperar la configuración completa.

El complemento de integración también puede definir parámetros secundarios que no aparecen en el asistente, pero puede modificarlos en **Configuración general** después de configurar la integración. Los valores predeterminados para los parámetros son suministrados por el plug-in o el sistema XProtect.

Conectar al sistema de control de acceso

Cuando el plug-in se ha integrado con éxito, aparece un resumen de la configuración del sistema de control de acceso recuperados. Revisar la lista para asegurarse de que todos los elementos se han integrado antes de continuar con el siguiente paso del asistente.

Cámaras asociadas

Mapear los puntos de acceso en el sistema de control de acceso con las cámaras del sistema XProtect, para mostrar vídeo relacionado a eventos de las puertas.

Podemos hacer que varias cámaras a un punto de acceso. El usuario XProtect Smart Client es entonces capaz de ver el vídeo de todas las cámaras en la investigación de los acontecimientos, por ejemplo.

El usuario XProtect Smart Client también es capaz de añadir una de las cámaras cuando se configura el **monitor del acceso** ver elementos.

Puertas con licencia están habilitadas de forma predeterminada. Desactive la casilla de verificación para desactivar una puerta y con ello liberar una licencia de puerta de control de acceso.

Resumen final

Su integración de sistemas de control de acceso se ha creado con éxito en XProtect con la configuración predeterminada heredados de la integración de plug-in. Los usuarios de clientes deben registrar en XProtect Smart Client para ver y utilizar el nuevo sistema de control de acceso.

Puede refinar la configuración si es necesario.

Propiedades de control de acceso

Pestaña Configuración general (control de acceso)

Nombre	Descripción
Habilitar	Los sistemas están habilitados de forma predeterminada, lo que significa que son visibles en XProtect Smart Client para los usuarios con derechos suficientes y que el sistema XProtect recibe eventos de control de acceso. Puede desactivar un sistema, por ejemplo durante el mantenimiento, para evitar crear alarmas innecesarias.
Nombre	El nombre de la integración del control de acceso tal como aparece en la Management Application y en los clientes. Puede sobrescribir el nombre existente por uno nuevo.
Descripción	Proporcionar una descripción de la integración de control de acceso. Esto es opcional.
Plug-in de integración	Muestra el tipo de sistema de control de acceso seleccionado durante la integración inicial.
Última actualización de configuración	Muestra la fecha y hora de la última vez que la configuración fue importada desde el sistema de control de acceso.
Configuración de Actualización	Haga clic en el botón cuando necesite para reflejar los cambios de configuración realizados en el sistema de control de acceso en XProtect, por ejemplo si ha añadido o eliminado una puerta. Aparece un resumen de los cambios en la configuración del sistema de control de acceso. Revise la lista para asegurarse de que su sistema de control de acceso se refleje correctamente antes de aplicar la nueva configuración.
Inicio de sesión requiere de un operador	Habilitar una entrada adicional para los usuarios del cliente, si el sistema de control de acceso es compatible con los derechos de usuario diferenciadas. Esta opción sólo está visible si el plug-in soporta la integración diferenciada derechos de usuario.

La denominación y el contenido de los campos siguientes son importados de la integración de plug-in. A continuación se presentan algunos ejemplos de campos típicos:

Nombre	Descripción
Dirección	Escriba la dirección del servidor que aloja el sistema de control de acceso integrado.
Puerto	Especificar el número de puerto en el servidor al que está conectado el sistema de control de acceso.
Nombre de usuario	Escriba el nombre del usuario, tal como se define en el sistema de control de acceso, que debe ser el administrador del sistema integrado de XProtect.

Nombre	Descripción
Contraseña	Especificar la contraseña para el usuario.

Las puertas y ficha Cámaras Asociadas (Control de acceso)

Esta ficha proporciona asignaciones entre los puntos de acceso de la puerta y cámaras, micrófonos o altavoces. Se asocia cámaras como parte del asistente de integración, pero se puede cambiar la configuración en cualquier momento. Asignaciones a los micrófonos y altavoces están implícitos a través del micrófono relacionado o representante de la cámara.

Nombre	Descripción
Puertas	Muestra una lista de los puntos de acceso de puertas disponibles definidas en el sistema de control de acceso, agrupados por la puerta. Para una navegación más fácil a las puertas correspondientes, se pueden filtrar en las puertas de su sistema de control de acceso con el cuadro de lista desplegable en la parte superior. **Habilitado**: Puertas con licencia están habilitadas de forma predeterminada. Puede deshabilitar una puerta para liberar una licencia. **Licencia**: Muestra si una puerta está disponible o si la licencia ha caducado. El campo está en blanco cuando la puerta está deshabilitada. **Eliminar**: Haga clic en **Quitar** para quitar una cámara de un punto de acceso. Si elimina todas las cámaras, la casilla de verificación para las cámaras asociadas se borra automáticamente.
Cámaras	Lista las cámaras configuradas en el sistema XProtect. Seleccione una cámara de la lista y arrastrarlo en el punto de acceso que corresponda a asociar el punto de acceso con la cámara.

Pestaña Eventos Control de acceso (Control de acceso)

Categorías de eventos que permiten a los eventos de grupo. La configuración de las categorías de eventos afecta al comportamiento de control de acceso en el sistema XProtect y le permite, por ejemplo, definir una alarma para disparar una sola alarma en varios tipos de eventos.

Nombre	Descripción
Evento de control de acceso	Muestra los eventos de control de acceso importados desde el sistema de control de acceso. La integración plug-in de los controles por defecto la activación y desactivación de los acontecimientos. Usted puede activar o desactivar eventos en cualquier momento después de la integración. Cuando se activa un evento, se almacena en la base de datos de eventos XProtect y es, por ejemplo, disponible para el filtrado en el XProtect Smart Client.
Tipo de fuente	Muestra la unidad de control de acceso que puede desencadenar el evento de control de acceso.

Nombre	Descripción
Categoría de evento	Asignar ninguna, una o más categorías de eventos a los eventos de control de acceso. El sistema asigna automáticamente las categorías de eventos correspondientes a los eventos durante la integración. Esto permite que la configuración por defecto en el sistema XProtect. Puede cambiar la asignación en cualquier momento. Incorporado en las categorías de eventos son: • Acceso denegado • Acceso permitido • Acceso requerido • Alarma • Error • Advertencia Eventos y categorías de eventos definidos por el plug-in de integración también aparecen, pero también se pueden definir sus propias categorías de eventos, consulte **categorías definidas por el usuario**. **Importante**: Si cambia las categorías de eventos en un sistema Corporate, asegurar que las reglas de control de acceso existentes siguen funcionando.
Categorías definidas por el usuario	Permite crear, modificar o eliminar categorías de eventos definidos por el usuario. Puede crear categorías de eventos cuando las categorías incorporadas no satisfacen sus necesidades, por ejemplo, en relación con la definición de eventos de activación para las acciones de control de acceso. Las categorías son globales para todos los sistemas de integración añadido al sistema XProtect. Permiten la creación de manejo entre sistemas, por ejemplo, en las definiciones de alarma. Si elimina una categoría de eventos definidos por el usuario, recibirá una advertencia si es utilizado por cualquier tipo de integración. Si elimina todos modos, todas las configuraciones hechas con esta categoría, por ejemplo, las acciones de control de acceso, ya no funcionan.

Pestaña de notificación de solicitud de acceso (Control de acceso)

Puede especificar las notificaciones de solicitud de acceso que aparecen en la pantalla de XProtect Smart Client cuando se produce un evento determinado.

Nombre	Descripción
Nombre	Introduzca un nombre para la notificación de solicitud de acceso.
Añadir notificación de solicitud de acceso	Haga clic para añadir y definir notificaciones de solicitud de acceso. Para eliminar una notificación, haga clic **X** en el lado derecho. Si un usuario de XProtect Smart Client inicia sesión en un sitio principal de una jerarquía Milestone Federated Architecture, notificaciones de solicitud de acceso de los sitios secundarios también aparecen en XProtect Smart Client.
Detalles de notificación de Solicitud de acceso	Establece qué cámaras, micrófonos o altavoces que aparecen en las notificaciones de solicitud de acceso cuando se produce un evento determinado. También debe especificar el sonido para alertar al usuario cuando la notificación aparece.
Añadir comandos	Seleccione el que los comandos que deben estar disponibles como botones en los cuadros de diálogo de notificación de solicitud de acceso en el XProtect Smart Client. Comandos de solicitud de acceso relacionados: • Permite a todos los comandos relacionados con el acceso operaciones de solicitud disponible en la unidad fuente. Por ejemplo **Puerta abierta**. Todos los comandos relacionados: • Permite a todos los comandos de la unidad fuente. Comando de control de acceso: • Permite a un comando de control de acceso seleccionado. Comando del sistema: • Permite a un comando predefinido en el sistema XProtect. Para eliminar un comando, haga clic **X** en el lado derecho.

Pestaña titulares de tarjetas (Control de acceso)

Usa los **titulares de la tarjeta** ficha para revisar la información sobre los titulares de tarjetas en el sistema de control de acceso.

Nombre	Descripción
Buscar titular de la tarjeta	Escribe los caracteres de un nombre de titular de la tarjeta y aparece en la lista, si es que existe.
Nombre	Muestra los nombres de los titulares de tarjetas recuperados del sistema de control de acceso.
Tipo	Lista el tipo de titular de la tarjeta, por ejemplo: • Empleado • Guardia • Huésped

Si el sistema de control de acceso admite la adición / eliminación de fotografías en el sistema XProtect, puede añadir imágenes a los titulares de tarjetas. Esto es útil si el sistema de control de acceso no incluye imágenes de los titulares de tarjetas.

Nombre	Descripción
Seleccione una fotografía	Especifique la ruta de un archivo con una imagen del titular de la tarjeta. Este botón no está visible si el sistema de control de acceso maneja las imágenes. Se admiten formatos de archivos son . bmp, . png y . jpg. Las imágenes se cambian de tamaño para maximizar la vista. Milestone recomienda que utilice una imagen cuadrática.
Eliminar imagen	Haga clic para borrar la imagen. Si el sistema de control de acceso tenía una imagen, esta imagen se muestra después de la eliminación.

Configurar peticiónes de acceso

Hay varios tipos de eventos de control de acceso, por ejemplo **Acceso denegado** y **Acceso otorgado**. Para habilitar las notificaciones de solicitudes de acceso, debe asociar el tipo de evento con la categoría de evento **Petición de acceso**. De forma predeterminada, **Acceso denegado** está asociado con **Petición de acceso**: Las notificaciones de solicitud de acceso se envían solo cuando se deniega el acceso a alguien. Para cambiar esta configuración, siga los pasos en este tema.

Requisitos:En los roles de los usuarios del cliente, debe habilitar las notificaciones. Para ello, en la función, haga clic en la ficha **Control de acceso** , seleccione **Control de acceso** y luego seleccione **Recibir notificaciones** casilla de verificación.

Pasos:

1. En el panel **Navegación del sitio**, seleccione **Control de acceso**.
2. En la ficha **Eventos del control de acceso**, en la columna **Evento del control de acceso**, ubique el tipo de evento que desea editar.

3. Para deshabilitar las solicitudes de acceso para un tipo de evento, en la columna **Categoría de evento** , haga clic en y limpiar el **Petición de acceso** casilla de verificación.
4. Para habilitar las solicitudes de acceso para un tipo de evento adicional, en la columna **Categoría de evento** , haga clic en y selecciona el **Petición de acceso** casilla de verificación.
5. Guardar los cambios.

XProtect LPR

Descripción del sistema de XProtect LPR

XProtect LPR (explicado)

Funcionalidad disponible depende del sistema que está utilizando. Ver la tabla de comparación de productos para obtener más información.

XProtect LPR ofrece análisis basado en el contenido de vídeo (VCA) y el reconocimiento de placas de matrícula de vehículos que interactúa con el sistema de vigilancia y su XProtect Smart Client.

Para leer los caracteres en una placa, XProtect LPR utiliza el reconocimiento óptico de caracteres en las imágenes ayudados por los ajustes de la cámara especializadas.

Se pueden combinar LPR (reconocimiento de matrículas) con otras funciones de vigilancia, como la grabación y la activación basada en eventos de salidas.

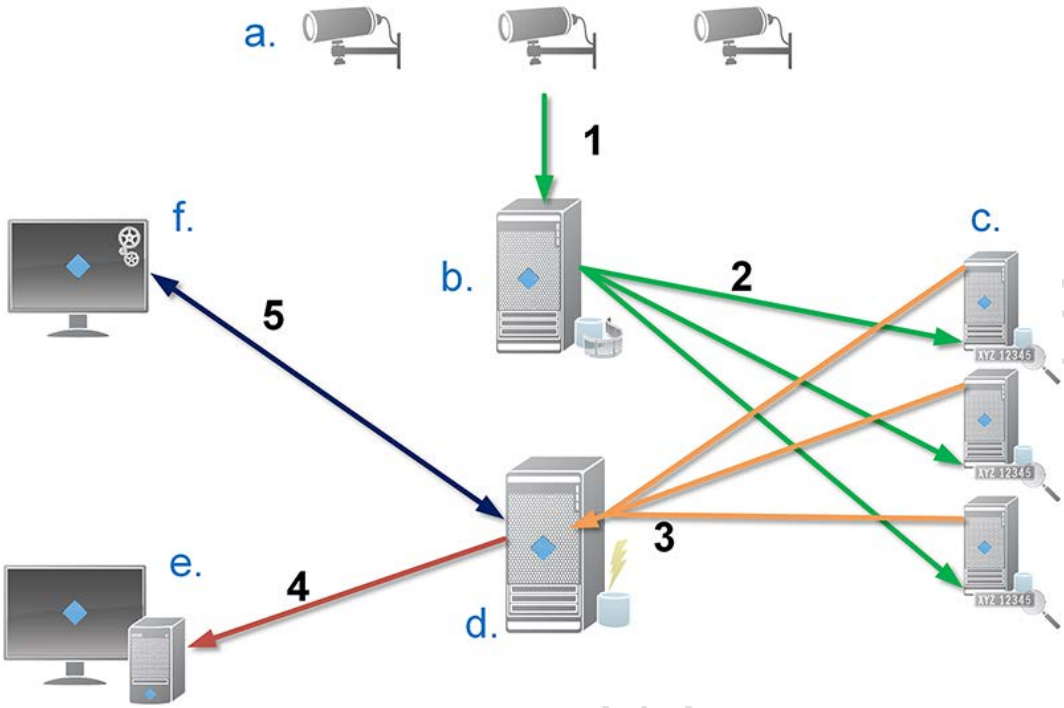
Ejemplos de eventos en XProtect LPR:

- Desencadenar grabaciones sistema de vigilancia en una calidad particular.
- Activar las alarmas.
- Hacer una pareja contra listas positivas / negativas de coincidencia de matrículas.
- Puertas abiertas.
- Encender las luces.
- Empuje video de incidentes a las pantallas de ordenador de los miembros del personal de seguridad particulares.
- Enviar mensajes de texto de teléfonos móviles.

Con un evento, puede activar alarmas en XProtect Smart Client.

Arquitectura del sistema XProtect LPR

Flujo de datos básica:



1. LPR (a) enviar video al servidor de grabación (b).
2. El servidor de grabación envía video a los servidores LPR (c) para reconocer placas de licencia comparándolas con las características de placa de matrícula en los módulos de país instalados.
3. Los servidores LPR envían reconocimientos al servidor de eventos (d) para que coincidan con las listas de coincidencias de matrículas.
4. El servidor de eventos envía eventos y alarmas para XProtect Smart Client (e) cuando existe una coincidencia.
5. El administrador del sistema gestiona toda la configuración LPR, por ejemplo, la configuración de eventos, alarmas y listas desde Management Client (f).

servidor LPR: El servidor LPR maneja el video LPR grabado por su sistema de vigilancia. Se analiza el vídeo y envía la información al servidor de eventos que lo utiliza para la activación de los eventos y alarmas definidas. Milestone recomienda instalar el servidor LPR en un equipo especialmente asignado para este propósito.

LPR cámara: La cámara LPR captura el video como cualquier otra cámara, pero algunas cámaras están dedicadas al uso de LPR. La cámara más adecuada que utilice, los reconocimientos más exitosos que van a recibir.

Módulo de país: Un módulo país es un conjunto de reglas que define placas de matrícula de un determinado tipo y la forma como perteneciente a un determinado país o región. Se dicta la placa y caracteres específicos, tales como el color, la altura, el espaciado y similares, que se utiliza durante el proceso de reconocimiento.

Lista de las matrículas: Una lista de coincidencias de matrículas es una lista definida por el usuario que ha creado. Las listas de coincidencia de matrículas son conjuntos de placas de matrícula que desea que su sistema para el tratamiento de una manera especial. Una vez que haya especificado una lista, puede configurar eventos para reconocer placas de matrícula en dichas listas y de esta manera eventos de disparo y alarmas.

Compatibilidad

XProtect LPR es compatible con la versión 2014 SP3 o más reciente de:

- XProtect Corporate
- XProtect Expert
- Milestone Husky™ M30
- Milestone Husky™ M50.

XProtect LPR es compatible con la versión 2017 R2 o posterior de:

- XProtect Professional+
- XProtect Express+

XProtect LPR es compatible con Milestone Husky M30 y Milestone Husky M50, pero actualmente estos productos no soportan la funcionalidad completa de XProtect LPR.

Requisitos mínimos del sistema

Para obtener información acerca de los requisitos mínimos del sistema para los diversos componentes de su sistema, vaya a la página web (https://www.milestonesys.com/support/resources/system-requirements) de Milestone.

Milestone recomienda instalar el servidor LPR en un equipo especialmente asignado para este propósito.

Licencias XProtect LPR

XProtect LPR requiere las siguientes licencias relacionadas con LPR:

- Una **licencia base** para XProtect LPR que cubre un número ilimitado de servidores LPR.
- One **Licencia de cámara LPR** por cámara LPR que desea utilizar en XProtect LPR.
- Una **licencia de módulo de país LPR** para cada país, estado o región que necesite en su solución XProtect LPR. **Cinco** licencias de módulo de país LPR se incluyen con la licencia base XProtect LPR. Todos los módulos de campo se instalan automáticamente al instalar el producto XProtect LPR. Sin embargo, los módulos instalados están deshabilitados por defecto y debe habilitar los módulos (ver "Pestaña modulos país" en la página 363) que desea utilizar. Sólo se pueden habilitar tantos módulos de país como los que tienen las licencias de módulo de país LPR.

Ejemplo: Tiene cinco licencias de módulo de país LPR y ha instalado 10 módulos de país. Una vez que haya seleccionado cinco módulos país, no se puede seleccionar más. Debe borrar algunos de sus selecciones antes de poder seleccionar otros módulos.

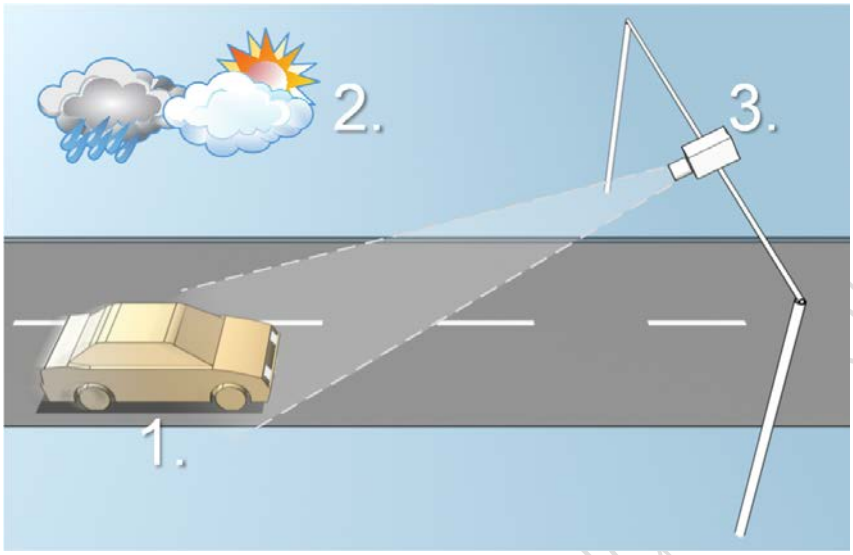
Para obtener información sobre el estado actual de sus licencias, consulte Ver información del servidor LPR (en la página 353).

Para comprar licencias adicionales relacionadas con LPR o módulos de país, póngase en contacto con su proveedor.

Preparación de cámaras para LPR (explicado)

LPR se diferencia de otros tipos de videovigilancia. Normalmente, se elige cámaras en función de su capacidad de proporcionar las mejores imágenes posibles para ser vistos por el ojo humano. Cuando elige cámaras para LPR, sólo es importante el área donde se espera detectar placas. Cuanto más claro y coherente capture una imagen en esa pequeña área, mayor será la tasa de reconocimiento que obtendrá.

Esta sección le ayuda a preparar las cámaras de reconocimiento de matrículas, pero también es una introducción a las teorías importantes sobre las cámaras y lentes que son cruciales para entender el fin de obtener imágenes óptimas.



Factores que influyen en la configuración de LPR:

1. Vehículo

- Velocidad
- Tamaño de la placa y la posición

2. Entorno físico

- Condiciones de iluminación
- Clima

3. Cámara

- Exposición
- Campo de visión
- Velocidad del Obturador
- Resolución
- Posicionamiento

Es importante tener en cuenta estos factores, ya que tienen una influencia crítica en el éxito del reconocimiento de la matrícula. Debe montar cámaras y configurar XProtect LPR de manera que coincida con cada entorno específico. No se puede esperar que el producto funcione correctamente sin necesidad de configuración. Una cámara utilizada para LPR tiene un consumo de CPU que es aproximadamente cinco veces mayor que una cámara normal. Si una cámara no se ha configurado correctamente, afectará en gran medida el nivel de reconocimientos exitosos y el rendimiento de la CPU.

Lea las siguientes secciones para conocer los factores que influyen en su solución LPR:

Posicionamiento de la cámara (en la página 341)

Angulos de camara (en la página 342)

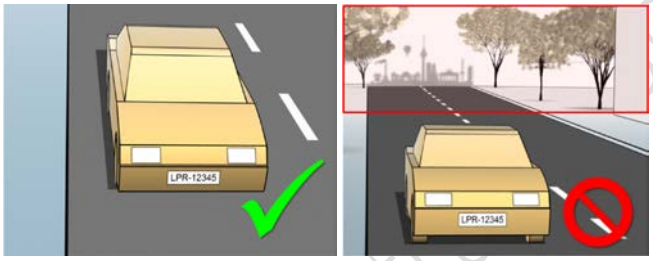
Recomendaciones ancho de la placa (en la página 343)

Posicionamiento de la cámara

Cuando monta cámaras para uso LPR, es importante tener una buena visión clara del área de interés para que la placa pueda ser detectada de forma consistente. Esto asegura el mejor rendimiento posible y bajo riesgo de detección falsa:

- El área debe cubrir **solamente** la parte de la imagen donde la matrícula es visible cuando el vehículo se mueve dentro y fuera de la imagen.
- Evitar tener objetos que bloquean la vista del camino de la cámara, tales como pilares, barreras, cercas, puertas.
- Evitar objetos en movimiento irrelevantes como las personas, los árboles, o la trata de

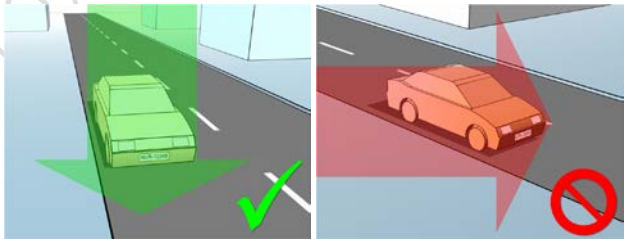
Si se incluyen demasiados elementos irrelevantes, interferirán en la detección y el servidor LPR utilizará los recursos de la CPU al analizar elementos irrelevantes en lugar de placas de licencia.



Para ayudarle a obtener una visión clara y sin molestias, se puede:

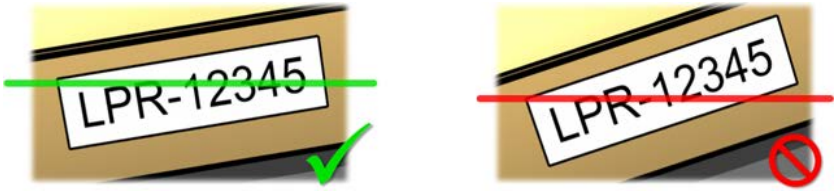
- Monte la cámara tan cerca como sea posible del área de interés.
- Ángulo de la cámara.
- Enfocar. Si se acerca, siempre utilizar el zoom óptico de la cámara.

Monte la cámara por lo que la placa de matrícula aparece desde la parte superior de la imagen (o inferior si el tráfico está alejando de la cámara) en lugar de desde el lado derecho o izquierdo. De esta manera se asegura que el proceso de reconocimiento de una placa de matrícula sólo se inicia cuando toda la placa está en la vista:

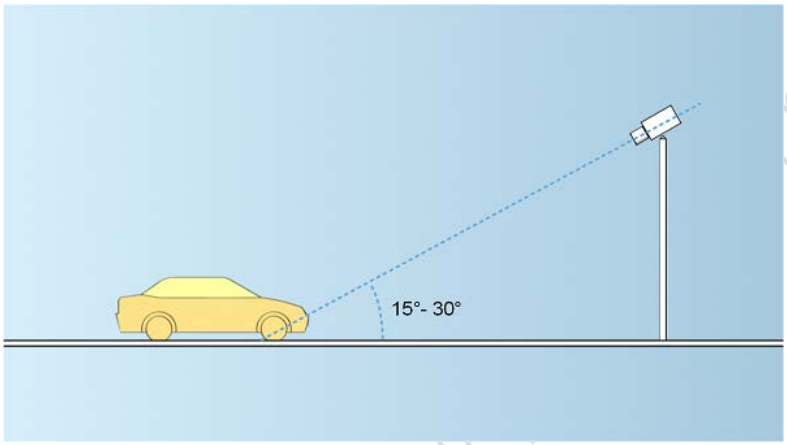


Angulos de camara

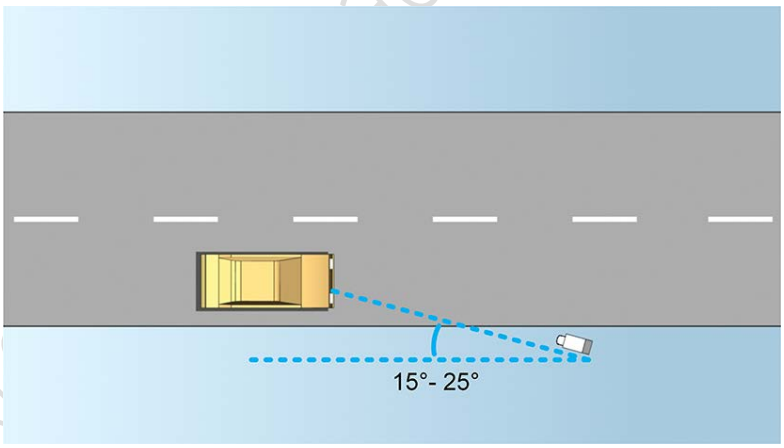
- **regla de una sola línea:** Monte la cámara de manera que se puede dibujar una línea horizontal que atraviesa tanto el borde izquierdo y derecho de la placa de matrícula en las imágenes capturadas. Consulte las siguientes ilustraciones para los ángulos correctos e incorrectos para el reconocimiento.



- **Ángulo vertical:** El ángulo de visión vertical recomendado de una cámara utilizada para LPR es entre 15 ° -30 °.

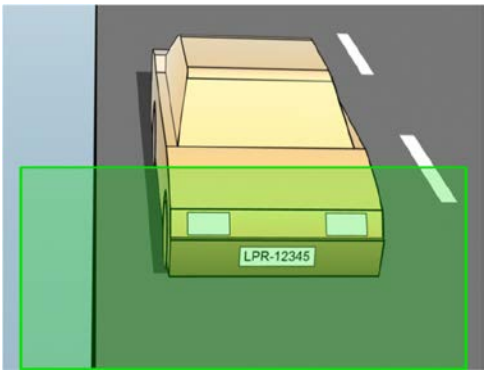


- **Ángulo horizontal:** El ángulo de visión horizontal máximo recomendado de una cámara utilizada para LPR es entre 15°-25°.



Recomendaciones ancho de la placa

Monte la cámara de manera que la instantánea ideal de la placa de matrícula es capturada cuando la placa de matrícula se encuentra en el centro o en la mitad inferior de la imagen:



Tomar una instantánea y asegúrese de que se cumplen los requisitos de ancho de trazo y ancho de la placa como se describe a continuación. Utilice un editor de gráficos estándar para medir la cantidad de píxeles. Al iniciar el proceso de alcanzar la anchura mínima de la placa, comenzar con una baja resolución en la cámara, y luego su forma de trabajo en una resolución más alta hasta que tenga la anchura de la placa requerida.

Anchura del trazo

El término píxeles por carrera se utiliza para definir un requisito mínimo para las fuentes que deben ser reconocidas. La siguiente ilustración describe lo que se entiende por trazos:

Debido a que el grosor de los trazos depende del país y el estilo de la placa, no se utilizan las mediciones como píxeles / cm o píxeles / pulgada.

La resolución para el mejor rendimiento LPR debe ser de al menos 2,7 píxeles / carrera.

Ancho de la placa

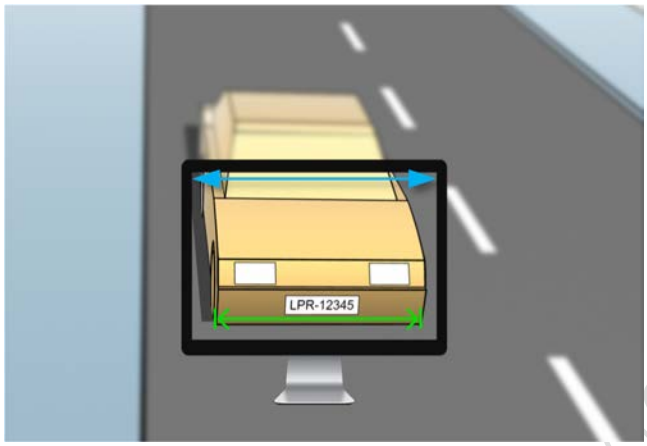
Tipo de la placa	Ancho de la placa	Configuración	El ancho mínimo de placa (píxeles)
Placas de Estados Unidos de una sola línea	• Anchura de placa de 12 pulgadas • trazo ancho alrededor de ¼ pulgadas	vehículos se detuvieron; sin entrelazado	130
		Los vehículos se mueven; entrelazado	215
Placas europeas de una sola línea	• Anchura de placa de 52 cm • anchura del trazo alrededor de 1 cm	vehículos se detuvieron; sin entrelazado	170
		Los vehículos se mueven; entrelazado	280

Si los vehículos se mueven cuando se registró, y se utiliza una cámara de entrelazado, sólo la mitad de la imagen se puede utilizar (sólo las líneas pares) para el reconocimiento en comparación con una cámara configurada para vehículos parados y sin entrelazado. Esto significa que los requisitos de resolución son casi el doble de alta.

Resolución de imagen

La calidad y la resolución de la imagen es importante para un éxito del reconocimiento de la matrícula. Por otro lado, si la resolución de vídeo es demasiado alta, la CPU puede estar sobrecargada con el riesgo de detecciones omitidos o defectuosas. Cuanto más bajo se puede configurar la resolución aceptable, la CPU mejor rendimiento y mayor tasa de detección que se obtiene.

En este ejemplo explicamos cómo hacer un cálculo de calidad de imagen simple y encontrar una resolución adecuada para LPR. El cálculo se basa en el ancho de un coche.



Estimamos que la anchura horizontal es de 200 cm / 78 pulgadas, como suponemos la anchura de un coche estándar es de 177 cm / 70 pulgadas, y además de eso añadimos ~ 10% para el espacio extra. También se puede hacer una medición física de la zona de interés, si lo que necesita saber la anchura exacta.

La resolución recomendada del espesor de trazo es 2,7 píxeles / trazo, y el espesor físico de trazo es de 1 cm de una placa europea y 0,27 pulgadas para una placa de Estados Unidos. Esto da el siguiente cálculo:

Cálculo de placas europeas en cm:

200 × 2,7 ÷ 1 = 540 pixeles

Solución recomendada = VGA (640 × 480)

Cálculo de placas de Estados Unidos en pulgadas:

78 × 2,7 ÷ 0,27 = 780 píxeles

Solución recomendada = SVGA (800 × 600)

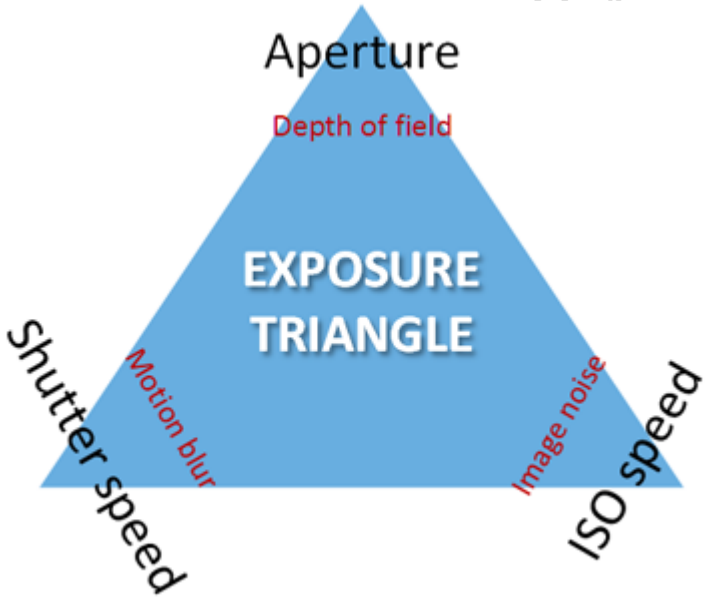
Debido a que las placas de los Estados Unidos usan una fuente con un trazo estrecho, se necesita una resolución más alta que para las placas europeos.

Resoluciones de vídeo comunes

Nombre	Píxeles (W x H)
QCIF	176×120
CIF	352×240
2CIF	704×240
VGA	640×480
4CIF	704×480
D1	720×576
SVGA	800×600
XGA	1024×768
720p	1280×1024

Comprensión de exposición de la cámara

Exposición de la cámara determina cómo luz / oscuridad y aguda / borrosa aparece una imagen cuando ha sido capturado. Esto está determinado por la configuración de tres cámaras: apertura del diafragma, velocidad de obturación y la sensibilidad ISO. La comprensión de su uso e interdependencia puede ayudarle a configurar la cámara correctamente para LPR.



Se pueden utilizar diferentes combinaciones de los tres parámetros para conseguir la misma exposición. La clave está en saber qué ventajas y desventajas de hacer, ya que cada ajuste también influye en los otros ajustes de la imagen:

Ajustes de cámara	Controles...	Afecta...
Abertura	La apertura ajustable que limita la cantidad de luz entre en la cámara	Profundidad de campo
Velocidad del Obturador	La duración de la exposición	El desenfoque de movimiento
La sensibilidad ISO	La sensibilidad del sensor de la cámara a una determinada cantidad de luz	Ruido de la imagen

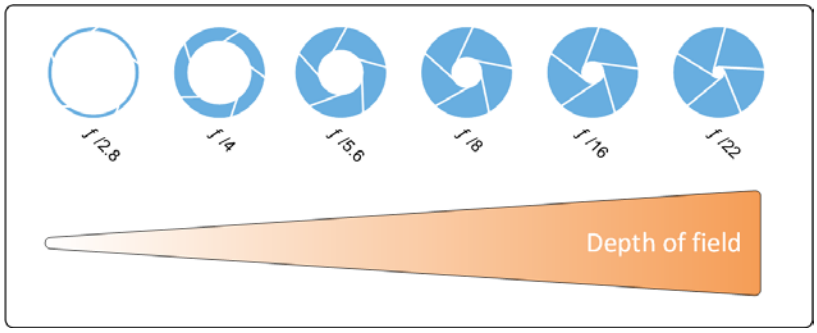
Las siguientes secciones describen cómo se especifica cada ajuste, lo que parece, y como un modo de exposición de la cámara dada afecta a esta combinación:

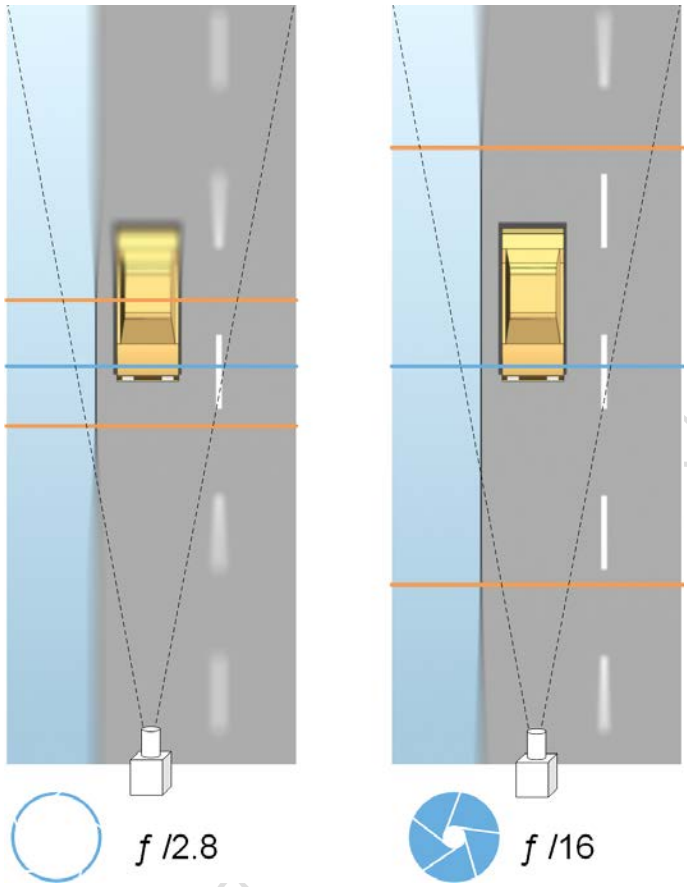
Los ajustes de apertura

El ajuste de apertura controla la cantidad de luz que entra en la cámara de la lente. Se especifica en términos de un valor de f-stop, que a veces puede ser contraintuitivo, porque el área de la apertura aumenta a medida que disminuye el f-stop.

Bajo valor de f-stop / abertura ancha = poca profundidad de campo

Alto valor de f-stop / abertura estrecha = gran profundidad de campo





El ejemplo ilustra cómo la profundidad de campo se ve afectada por el valor f-stop. La línea azul indica el punto de enfoque.

Un alto valor de f-stop permite tener una distancia más larga donde la matrícula está enfocada. Las buenas condiciones de luz son importantes para una exposición suficiente. Si las condiciones de iluminación son insuficientes, el tiempo de exposición debe ser mayor, lo que aumenta el riesgo de obtener imágenes borrosas.

Un valor bajo de f-stop reduce el área de enfoque y por lo tanto el área utilizada para el reconocimiento, pero es adecuado para condiciones de baja luz. Si es posible garantizar que los vehículos están pasando la zona de enfoque a baja velocidad, un valor bajo de diafragma es adecuado para un reconocimiento constante.

Velocidad del Obturador

Un obturador de cámara determina cuando el sensor de la cámara está abierta o cerrada para la luz entrante de la lente de la cámara. La velocidad de obturación se refiere a la duración cuando el obturador está abierto y

la luz puede entrar en la cámara. La velocidad de obturación y el tiempo de exposición se refieren al mismo concepto, y una velocidad de obturación más rápida significa un tiempo de exposición más corto.

El desenfoque de movimiento no es deseado para el reconocimiento y la vigilancia de matrículas. En muchas ocasiones, los vehículos están en movimiento, mientras que las placas se detectan lo que hace que una velocidad de obturación correcta es un factor importante. La regla de oro es mantener la velocidad de obturación lo suficientemente alto como para evitar el desenfoque de movimiento, pero no demasiado alto ya que esto puede hacer que las imágenes subexpuestas en función de la luz y la abertura.

La sensibilidad ISO

La velocidad ISO determina la sensibilidad de la cámara a la luz entrante. Similar a la velocidad de obturación, sino que también se correlaciona 1: 1 con la cantidad de los aumentos de exposición o disminuye. Sin embargo, a diferencia de abertura y velocidad de obturación, una velocidad ISO más baja es en general deseable, ya velocidades ISO más altas aumentan drásticamente el ruido de la imagen. Como resultado, la velocidad ISO está por lo general sólo aumentó de su valor mínimo si la calidad de imagen deseada no se pueda obtener mediante la modificación de los ajustes de apertura y velocidad de obturación únicamente.

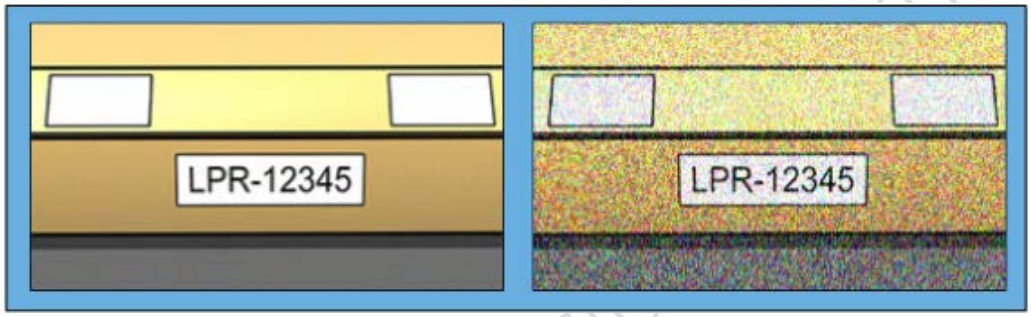


Imagen de baja velocidad ISO Imagen de alta velocidad ISO

Las velocidades ISO más comunes son 100, 200, 400 y 800, aunque muchas cámaras también permiten que los valores inferiores o superiores. Con digital réflex de lente única (DSLR), un rango de 50-800 (o superior) a menudo es aceptable.

Entorno físico

Cuando monte y utilice cámaras para LPR, tenga en cuenta los siguientes factores relacionados con el entorno:

- **Mucha luz:** El exceso de luz en el entorno puede conducir a la sobreexposición o manche.
  - **Sobreexposición** es cuando las imágenes se exponen a demasiada luz, lo que resulta en un aspecto quemado y demasiado blanco. Para evitar la sobreexposición, Milestone recomienda que utilice una cámara con un alto rango dinámico y / o utilizar una lente auto-iris. **Iris** es la apertura ajustable. Por esa razón, iris tiene un efecto significativo sobre la exposición de las imágenes.

- **Frotis** es un efecto que lleva a la luz indeseada líneas verticales en las imágenes. A menudo es causada por leves imperfecciones de dispositivo de carga acoplada de las cámaras (CCD) de imágenes. Las cámaras de CCS son los sensores que se utilizan para crear digitalmente las imágenes.

- **poca luz:** Muy poca luz en el entorno o demasiado poca iluminación externa puede conducir a la subexposición.

  - **Poca exposición** es cuando las imágenes se exponen a muy poca luz, lo que resulta en una imagen oscura con apenas contraste (en la página 350). Cuando auto-ganancia (ver "Características de la cámara no deseados" en la página 351) no se puede desactivar o cuando no se puede configurar un máximo permitido tiempo de obturación (ver "Lente y velocidad de obturación" en la página 349) para la captura de vehículos en movimiento, muy poca luz inicialmente conducir a ganar ruido y desenfoque de movimiento en las imágenes y, finalmente, a subexposición. Para evitar la subexposición, utilice suficiente iluminación externa y / o utilizar una cámara que tiene suficiente sensibilidad en entornos de poca luz sin utilizar la ganancia.

- **infrarrojos:** Otra forma de superar las condiciones de iluminación difíciles es utilizar iluminación infrarroja artificial combinado con una cámara sensible al infrarrojo con un filtro de paso de infrarrojos. Placas de matrícula retrorreflectantes son especialmente adecuados para su uso con iluminación infrarroja.

  - **La retro-reflectividad** se logra cubriendo las superficies con un material reflectante especial que envía una gran parte de la luz de una fuente de luz recta hacia atrás a lo largo del camino de donde procede. Objetos retrorreflectantes parecen brillar mucho más brillantes que otros objetos. Esto significa que por la noche se pueden ver claramente desde distancias considerables. Retro-reflectividad se usa con frecuencia para señales de tráfico, y también se utiliza para diferentes tipos de placas de matrícula.

- **El tiempo:** Nieve o la luz del sol de mayo muy brillante, por ejemplo, requieren una configuración especial de las cámaras.

- **Estado de la platina:** Los vehículos pueden haber dañado o placas sucias. A veces esto se hace deliberadamente en un intento de evitar el reconocimiento.

Lente y velocidad de obturación

Al configurar las lentes de las cámaras y las velocidades de obturación para LPR, tenga en cuenta lo siguiente:

- **Foco:** Siempre asegúrese de que la placa de matrícula está en el foco.

- **Auto-iris:** Si se utiliza una lente de iris automático, ajustar el enfoque con la abertura lo más abierto posible. Con el fin de hacer que el diafragma abierto, puede utilizar filtros (ND) de densidad neutra o, si

la cámara es compatible con la configuración manual de la hora del tiempo de obturación del obturador se puede establecer en un tiempo muy corto.

- **Densidad neutra** (ND) filtros o filtros de color gris, básicamente, reducir la cantidad de luz que entra en una cámara. Trabajan como "gafas de sol" para la cámara. Los filtros ND afectan a la exposición de imágenes (ver "Comprensión de exposición de la cámara" en la página 345).

- **infrarrojos:** Si se utiliza una fuente de luz infrarroja, el enfoque puede cambiar cuando se cambia entre la luz visible y la luz infrarroja. Puede evitar el cambio de enfoque mediante el uso de una lente compensada por infrarrojos, o mediante el uso de un filtro de paso de infrarrojos. Tenga en cuenta que si se utiliza un filtro de paso de infrarrojos, es una fuente de luz infrarroja requiere -también durante el día.

- **Velocidad del vehículo:** Cuando los vehículos están en movimiento, tiempo de obturación cámaras 'debe ser lo suficientemente corto para evitar el desenfoque de movimiento. Una fórmula para el cálculo del tiempo de obturación adecuado más largo es:

  - **Velocidad del vehículo en km/h:** Tiempo de exposición en segundos = 1 segundos / (11 x max velocidad del vehículo en kilómetros por hora)

  - **Velocidad del vehículo en mph:** Tiempo de exposición en segundos = 1 segundos / (18 x max velocidad del vehículo en millas por hora)

  donde / denota "dividido por" y × denota "multiplicado por".

La siguiente tabla proporciona directrices para velocidades de obturación recomendadas cámara para diferentes velocidades del vehículo:

Tiempo de obturación en segundos	Max. la velocidad del vehículo en kilómetros por hora	Max. Velocidad del vehículo en millas por hora
1/50	4	2
1/100	9	5
1/200	18	11
1/250	22	13
1/500	45	27
1/750	68	41
1/1000	90	55
1/1500	136	83
1/2000	181	111
1/3000	272	166
1/4000	363	222

Contraste

Cuando determine el contraste correcto para su cámara LPR, considere la diferencia en el valor de gris (cuando las imágenes se convierten en escala de grises de 8 bits) entre los caracteres de la placa y el color de fondo de la placa:

Buen contraste

Contraste aceptable; reconocimiento es todavía posible

Píxeles de una imagen en escala de grises de 8 bits pueden tener valores de color que van de 0 a 255, donde el valor de escala de grises 0 es negro absoluto y 255 es blanco absoluto. Al convertir su imagen de entrada a una imagen en escala de grises de 8 bits, la diferencia mínima entre el valor de píxel de un píxel en el texto y un píxel en el fondo debe ser de al menos 15.

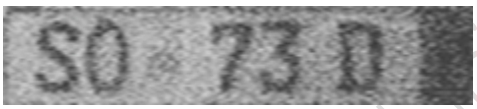
Tenga en cuenta que ruido en la imagen (ver "Características de la cámara no deseados" en la página 351), el uso de la compresión (ver "Características de la cámara no deseados" en la página 351), las condiciones de luz, y similares puede hacer que sea difícil determinar los colores de los caracteres y el fondo de una placa de matrícula.

Características de la cámara no deseados

Cudo configura cámaras para LPR, tenga en cuenta lo siguiente:

Ajuste automático de ganancia: Uno de los tipos más comunes de interferencia de la imagen causada por las cámaras es la ganancia de ruido.

- **Ganancia** es básicamente la forma en que una cámara captura una imagen de una escena y distribuye luz en ella. Si la luz no se distribuye de manera óptima en la imagen, el resultado es el ruido de ganancia.

  El control de ganancia requiere que se aplican algoritmos complejos, y muchas cámaras tienen características para el ajuste automático de ganancia. Desafortunadamente, estas características rara vez son útiles en relación con LPR. Milestone recomienda que configure la funcionalidad de ganancia automática de sus cámaras para que sea lo más baja posible. Alternativamente, deshabilitar la función de ganancia automática de las cámaras.

  En un entorno oscuro, se puede evitar el ruido de la ganancia mediante la instalación de alumbrado exterior suficiente.

Mejora automática: Algunas cámaras utilizan curvas de nivel, de borde o de mejora de contraste algoritmos para hacer que las imágenes se vean mejor para el ojo humano. Tales algoritmos pueden interferir con los algoritmos utilizados en el proceso LPR. Milestone recomienda desactivar las cámaras 'de contorno, borde y algoritmos de mejora de contraste siempre que sea posible.

Compresión automática: Las altas tasas de compresión pueden tener una influencia negativa sobre la calidad de las imágenes de placas de matrícula. Cuando se utiliza una tasa de compresión alta, se necesita más resolución (ver "Recomendaciones ancho de la placa" en la página 343) para lograr un rendimiento LPR óptimo. Si se utiliza una compresión JPEG baja, el impacto negativo en LPR es muy bajo, siempre que las imágenes se guarden con un nivel de calidad JPEG de 80% o superior y las imágenes tengan resolución, contraste y enfoque normales, así como un bajo nivel de ruido nivel.

La imagen de la matrícula guardado con un nivel de calidad de JPEG de 80% (es decir, baja compresión); aceptable.	La imagen de la matrícula guardado con un nivel de calidad de JPEG de 50% (es decir, alta compresión); inaceptable

Instalación XProtect LPR

Instalar XProtect LPR

Para ejecutar XProtect LPR, debe instalar:

- Al menos un servidor LPR.
- El complemento XProtect LPR en todos los equipos que ejecutan Management Client y el servidor de eventos.
- Asegúrese de que el usuario seleccionado para ejecutar el servicio del servidor LPR puede tener acceso al servidor de administración.

Milestone recomienda que noinstale el servidor LPR en el mismo equipo que su servidor de administración o servidores de grabación.

Iniciar la instalación:

1. Ir a la página de descarga en el sitio web (http://www.milestonesys.com/downloads) de Milestone.
2. Descargar los dos instaladores:
   - Milestone XProtect LPR Plug-in instalador en todos los equipos que ejecutan Management Client y el servidor de eventos.
   - Milestone XProtect LPR Servidor instalador para todos los equipos asignados para este propósito. También puede crear servidores virtuales para LPR en un equipo.
3. En primer lugar, ejecute todas las instaladoras Milestone XProtect LPR Plug-in.
4. A continuación, ejecute instalador(es) Milestone XProtect LPR Server.

   Durante la instalación, especifique la dirección IP o el nombre de host del servidor de gestión o del servidor de imágenes, incluido el nombre de usuario del dominio y la contraseña de una cuenta de usuario que tenga derechos de administrador del sistema de vigilancia.
5. Inicie el Management Client.

   En **Panel Navegación del sitio**, su Management Client lista automáticamente los servidores LPR instalados en la lista **LPR Servidores** .
6. Asegúrese de que tiene las licencias necesarias (ver "Licencias XProtect LPR" en la página 339).
7. Todos los módulos de campo se instalan automáticamente al instalar el producto XProtect LPR. Sin embargo, los módulos instalados están deshabilitados por defecto y debe habilitar los módulos (ver "Pestaña modulos país" en la página 363) que desea utilizar. Sólo se pueden habilitar tantos módulos de país como los que tienen las licencias de módulo de país LPR.

No puede agregar servidores LPR desde Management Client.

Si necesita instalar más servidores LPR después de la instalación inicial, ejecute el instalador Milestone XProtect LPR Server en estos servidores.

Si un programa antivirus está instalado en un equipo que ejecuta el software XProtect, es importante que se excluye la carpeta C:\ProgramData\Milestone\XProtect LPR. Sin la aplicación de esta excepción, la detección de virus utiliza una cantidad considerable de recursos del sistema y el proceso de digitalización puede bloquear temporalmente los archivos.

Actualiza XProtect LPR

Para actualizar XProtect LPR, siga los mismos pasos que para la instalación (ver "Instalar XProtect LPR" en la página 352).

Si actualiza desde XProtect LPR 1.0 a XProtect LPR 2016, algunos ajustes de reconocimiento no son compatibles con los de la configuración anterior. Para aplicar la nueva configuración, debe guardar su configuración. Los ajustes que previamente le ha permitido voltear, rotar e invertir los colores del vídeo se han eliminado. Si aún necesita estas funciones, se debe cambiar la configuración de las propias cámaras.

Configuración XProtect LPR

Ver información del servidor LPR

Para comprobar el estado de los servidores LPR:

1. En el **Panel Navegación del sitio**, expanda **Servidores** y seleccione **servidores LPR**. Ir al panel general.

   Se abre la ventana **de la información del servidor LPR** con un resumen del estado del servidor:

   - Nombre
   - Nombre de host
   - Estado

2. Seleccione el servidor LPR relevante y revise todos los detalles para este servidor (ver "Propiedades de información del servidor LPR" en la página 353).

Propiedades de información del servidor LPR

Campo	Descripción
Nombre	Aquí puede cambiar el nombre del servidor LPR.
Nombre de host	Muestra el nombre de host del servidor LPR. La primera parte del nombre del servidor LPR consiste en el nombre del equipo host para la instalación del servidor LPR. Ejemplo: MYHOST.domainname.country .

Campo	Descripción
Estado	Muestra el estado del servidor LPR. Si el servidor acaba de ser añadido, la situación es la siguiente: • No hay cámaras LPR configuradas. Si el sistema está funcionando sin problemas, la situación es la siguiente: • Todas las cámaras LPR están funcionando. Como alternativa, el sistema vuelve: • El servicio no está respondiendo. • No está conectado al sistema de vigilancia. • El servicio no está funcionando. • Servidor de eventos no está conectado. • Error desconocido. • X de Y LPR cámaras funcionando.
Tiempo de Servicio	Muestra el tiempo de espera desde que el servidor LPR estuvo inactivo y el servicio del servidor LPR se inició.
Uso de la CPU del ordenador	Muestra el uso actual de la CPU en todo el equipo con los servidores LPR instalados.
Memoria disponible	Muestra la cantidad de memoria disponible en el servidor LPR.
Matrículas reconocidas	Muestra el número de placas que el servidor LPR ha reconocido en esta sesión.
Cámaras LPR	Muestra una lista de cámaras LPR habilitadas que se ejecutan en el servidor LPR y su estado.
Cámaras LPR disponibles	Según su licencia, este número muestra cuántas cámaras LPR adicionales se le permite agregar y utilizar en todos sus servidores LPR en total.
Módulos disponibles de los países	Según su licencia, este número muestra cuántos módulos adicionales de país se pueden utilizar en todos los servidores LPR en total. También incluye el número de módulos de países que ya están en uso.

Configuración de cámaras para LPR

Requisitos para LPR en el Management Client

Una vez que las cámaras han sido montadas y agregadas en el Management Client, ajuste los ajustes de cada cámara para que coincidan con los requisitos para LPR. Ajusta la configuración de la cámara en las fichas de propiedades de cada dispositivo de la cámara.

Para las cámaras pertinentes, Milestone recomienda:

- Establecer el códec de vídeo a formato JPEG.

Tenga en cuenta que si utiliza codec H.264 o H.265, sólo los fotogramas clave son compatibles. Esto suele ser sólo un cuadro por segundo que no es suficiente para LPR. Para velocidades de fotogramas más altas, utilice siempre un códec JPEG.

- Especificar una velocidad de cuatro fotogramas por segundo.
- Evitar la compresión, por lo que establecer una buena calidad.
- Si es posible, especificar una resolución por debajo de un megapíxel.
- Si es posible, mantener la nitidez automática en un nivel bajo.

Para aprender sobre los fundamentos de LPR, familiarícese con la información en Preparación de cámaras para LPR (explicado) (en la página 340).

Instantáneas (explicadas)

El sistema utiliza instantáneas para optimizar la configuración de forma automática y para visualizar el efecto de la configuración de reconocimiento ya que se aplican.

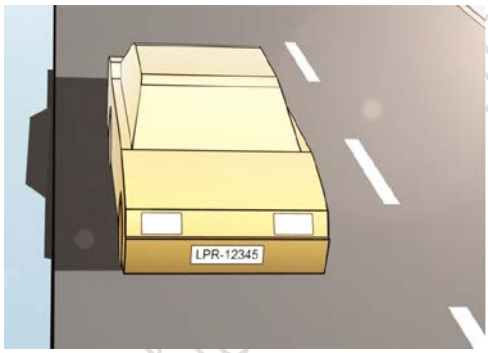
Es necesario proporcionar al menos una instantánea válida con el fin de completar la configuración inicial de una cámara.

Como pauta, capturar instantáneas de los vehículos en el entorno y las condiciones físicas reales, en los que desea ser capaz de reconocer las matrículas.

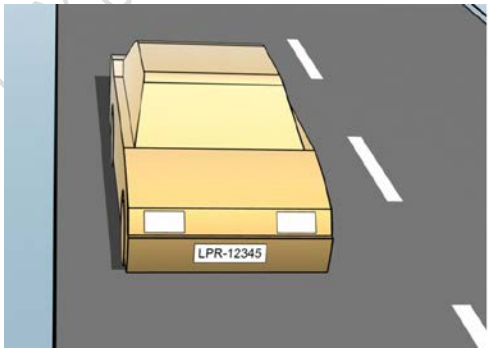
La lista siguiente muestra ejemplos de las situaciones que se deben considerar cuando se captura y seleccionar las instantáneas. No todos pueden ser aplicables a su entorno.

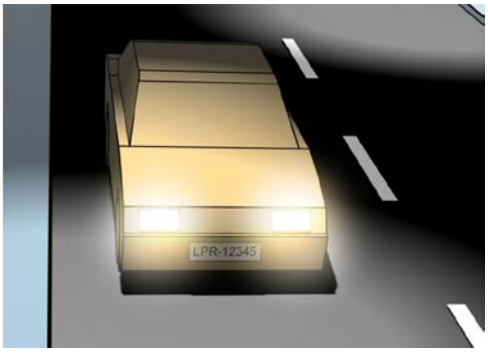
Milestone recomienda seleccionar mínimos 5-10 instantáneas que representan las condiciones típicas de:

- **El clima; por ejemplo, la luz del sol y la lluvia**

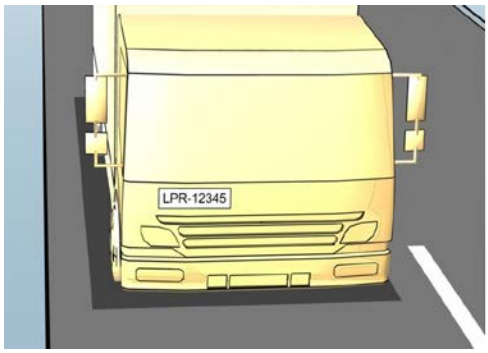


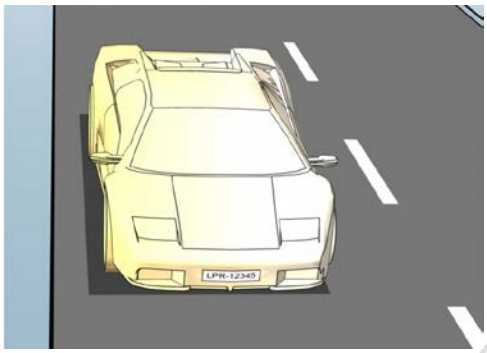
- **La luz; por ejemplo, luz del día y noche**



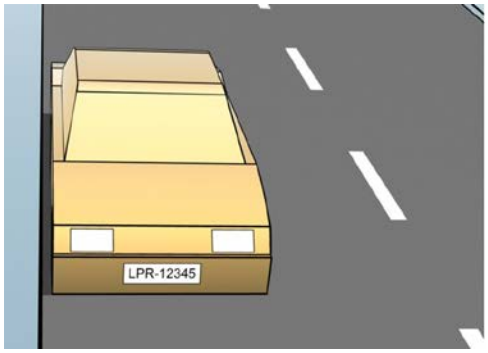


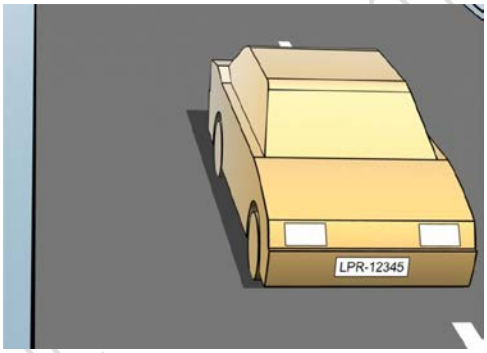
- **Tipos de vehículos; para definir la parte superior e inferior del área de reconocimiento**



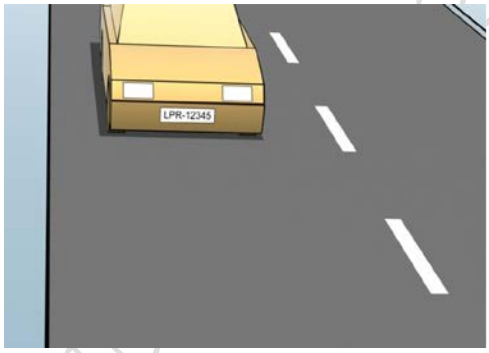


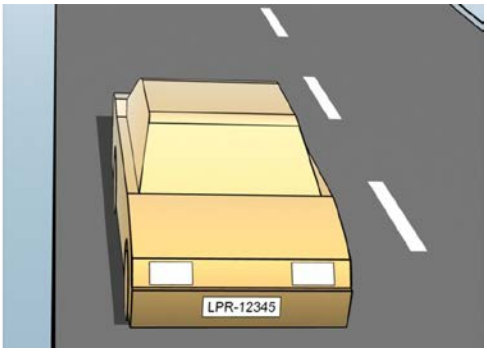
- **Posición en el pasillo; para definir la izquierda ya la derecha del área de reconocimiento**





- **Distancia al coche; Para definir el área donde LPR analiza las matrículas**





Añadir cámara LPR

Para configurar las cámaras para LPR, ejecuta inicialmente el **Añadir cámara LPR** asistente. El asistente le guiará a través de los principales pasos de configuración y optimiza automáticamente la configuración.

Para ejecutar el asistente:

1. En el **Panel Navegación del sitio**, expanda **Servidores**, expanda **Servidores LPR** y seleccione **LPR cámara**.

2. Ir al panel general. Hacer clic con el botón derecho **LPR cámara**.
3. En el menú que aparece, seleccione **Añadir la cámara LPR** y siga las instrucciones del asistente:
   - Seleccione la cámara que desea configurar para LPR.
   - Seleccione los módulos de país que desea utilizar con su cámara LPR (ver "Pestaña modulos país" en la página 363).
   - Seleccionar instantáneas para usar para validar la configuración (ver "Instantáneas (explicadas)" en la página 355).
   - Validar el resultado del análisis instantánea (ver "Validar configuración" en la página 365).
   - Seleccione qué lista de matrículas de placas para utilizar (ver "Listas de matrículas (explicadas)" en la página 366). Seleccione la opción predeterminada, si usted todavía no ha creado ninguna lista.
4. En la última página, haga clic en **Cerrar**.

   La cámara LPR aparece en Management Client y en función de sus selecciones, el sistema ha optimizado la configuración de reconocimiento para la cámara (ver "Pestaña de configuración reconocimiento" en la página 358).
5. Seleccione la cámara que haya agregado y revisar su configuración. Sólo se necesita cambiar la configuración si el sistema no reconoce placas de circulación, así como se espera.
6. En la pestaña **programación de reconocimiento**, haga clic en Validar configuración (en la página 365).

Ajuste los ajustes de la cámara LPR

El sistema optimizó automáticamente la configuración de su cámara LPR, cuando agregó la cámara LPR con el **Añadir cámara LPR** asistente. Si desea realizar cambios en la configuración inicial, se puede:

- Cambiar el nombre del servidor o cambiar el servidor (ver "Pestaña Info" en la página 357)
- Ajustar y validar los ajustes de reconocimiento (ver "Pestaña de configuración reconocimiento" en la página 358)
- Añadir más listas de concordancia de matrículas (ver "Pestaña Lista de coincidencias" en la página 362)
- Habilitar módulos de país adicionales (ver "Pestaña modulos país" en la página 363)

Pestaña Info

Esta pestaña ofrece información sobre la cámara seleccionada:

Nombre	Descripción
Habilitar	Las cámaras LPR se habilitan de forma predeterminada después de la configuración inicial. Desactive cualquier cámara que no se utilice en conexión con LPR. La desactivación de una cámara LPR no impide que realice una grabación normal en el sistema de vigilancia.
Cámara	Muestra el nombre de la cámara seleccionada tal como aparece en el XProtect Management Client y los clientes.

Nombre	Descripción
Descripción	Utilice este campo para introducir una descripción (opcional).
Cambiar servidor	Haga clic para cambiar el servidor LPR. Cambiar el servidor LPR puede ser una buena idea si necesita balance de carga. Por ejemplo, si la carga de la CPU es demasiado alta en un servidor LPR, Milestone recomienda mover una o más cámaras LPR a otro servidor LPR.

Pestaña de configuración reconocimiento

Cambie la configuración de reconocimiento manualmente. Con base en las instantáneas que proporcionó, el sistema configuró automáticamente la configuración de reconocimiento. Cambiar estos ajustes puede afectar en gran medida la tasa de éxito del reconocimiento.

Los botones de acción

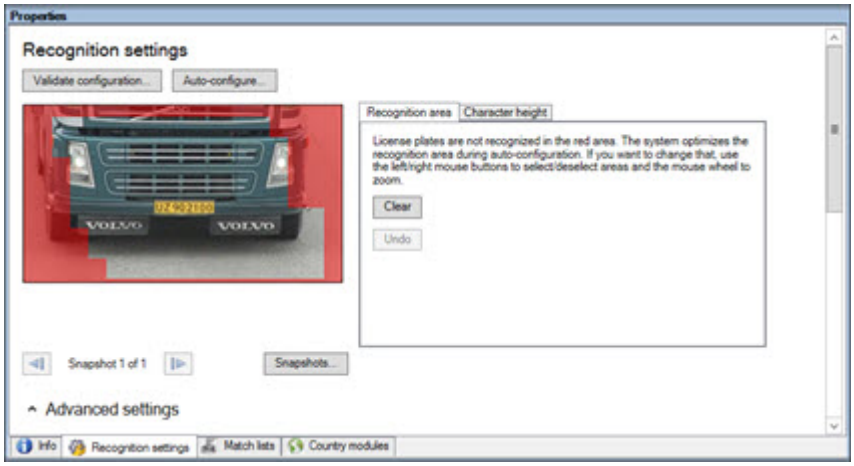
Cambiar, actualizar y validar configuraciones configuradas automáticamente.

Nombre	Descripción
Validar configuración	Prueba que la licencia placas se reconocen como se esperaba (ver "Validar configuración" en la página 365).
Configuración automática	Descarte los cambios manuales y configuraciones de configuración automática (ver "Configuración automática" en la página 365).
Instantáneas	Añadir o eliminar instantáneas (ver "Seleccionar instantáneas" en la página 364).

Área de reconocimiento

Para garantizar el mejor rendimiento y evitar los reconocimientos falsos, Milestone recomienda seleccionar un área de reconocimiento claramente definida y "bien recortada". El área debe cubrir solamente la parte de la imagen donde la placa de la licencia es visible y permanece visible mientras que el vehículo se mueve dentro y fuera de la imagen. Evite objetos móviles irrelevantes (personas, árboles, tráfico) en el área de reconocimiento (ver "Posicionamiento de la cámara" en la página 341) .

Las placas de matrícula no se reconocen en la zona roja.



Al especificar un área de reconocimiento, puede hacer clic en:

- **Borrar** para eliminar todas las selecciones y seleccionar nuevas áreas para LPR.
- **Deshacer** para volver al último área de reconocimiento guardada.

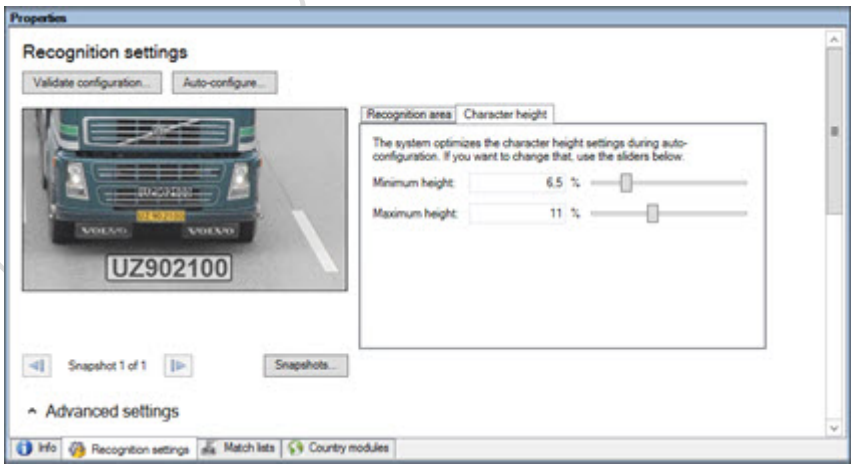
Después de cambiar la configuración de su cámara LPR, validar su configuración (ver "Validar configuración" en la página 365) para comprobar si el sistema reconoce placas de la licencia, así como se espera.

Altura de los caracteres

Defina la altura mínima y máxima de los caracteres de la placa (en porcentaje). Seleccione altura de los caracteres lo más cerca posible a la altura de los caracteres de la matrícula real.

Estos ajustes de caracteres afectan el tiempo y el proceso de reconocimiento. Cuanto menor sea la diferencia entre la altura mínima y la máxima del carácter:

- El proceso LPR es más suave.
- Cuanto menor sea la carga de la CPU.
- Cuanto antes obtenga los resultados.



La superposición en la instantánea muestra el ajuste de altura de carácter definido actualmente. La superposición crece y se contrae proporcionalmente a la configuración de altura de caracteres a la derecha.

Para facilitar la comparación, arrastre la superposición encima de la placa de matrícula real en la instantánea. Zoom con la rueda del ratón para una mirada más cercana.

Nombre	Descripción
Altura mínima	Establezca la altura mínima de caracteres para incluir placas en el proceso de reconocimiento. Si los caracteres reales de la placa son menores que el valor especificado, el sistema no iniciará el proceso de reconocimiento.
Altura máxima	Establezca la altura máxima de caracteres para incluir placas en el proceso de reconocimiento. Si los caracteres reales de la placa son mayores que el valor especificado, el sistema no iniciará el proceso de reconocimiento.

Después de cambiar la configuración de su cámara LPR, validar su configuración (ver "Validar configuración" en la página 365) para comprobar si el sistema reconoce placas de la licencia, así como se espera.

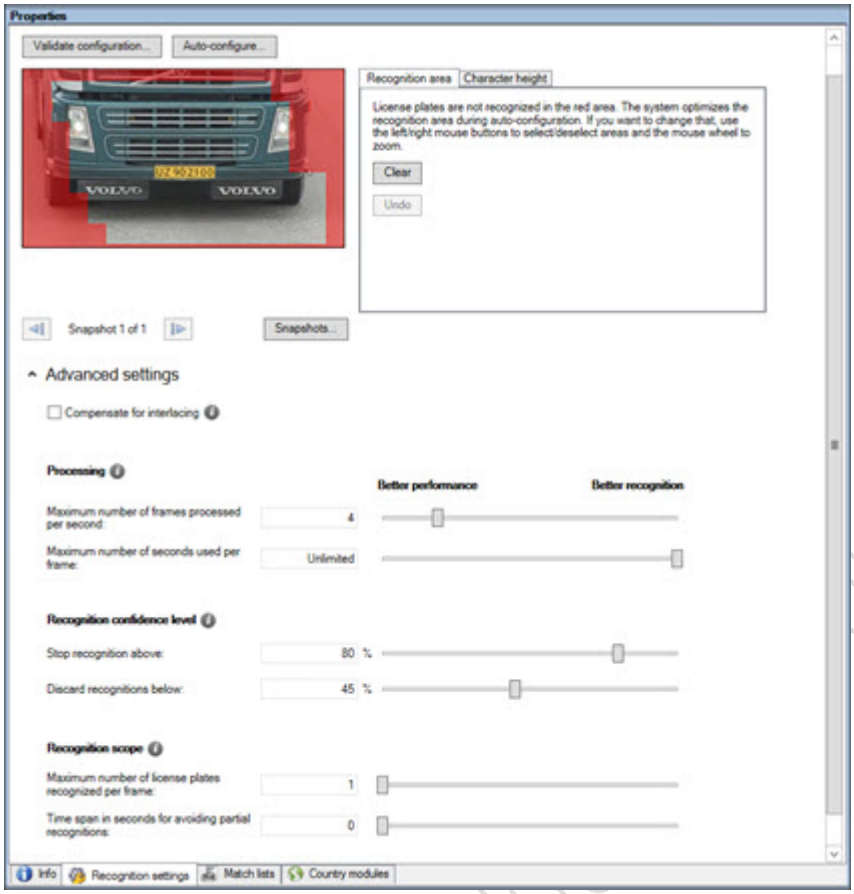
Ajustes avanzados

El proceso de reconocimiento tiene dos pasos: 1) encontrar la (s) placa (s) y 2) reconocer los caracteres en las placas. Haga clic en **Configuración avanzada** para definir un equilibrio entre velocidad de procesamiento y calidad de reconocimiento.

Alta calidad de reconocimiento:

- necesita un mayor esfuerzo computacional.
- aumenta la carga de la CPU.

- tarda más tiempo en devolver los resultados.



El proceso de reconocimiento se detiene cuando se cumplen los resultados óptimos y devuelve la placa que reconoció en ese momento.

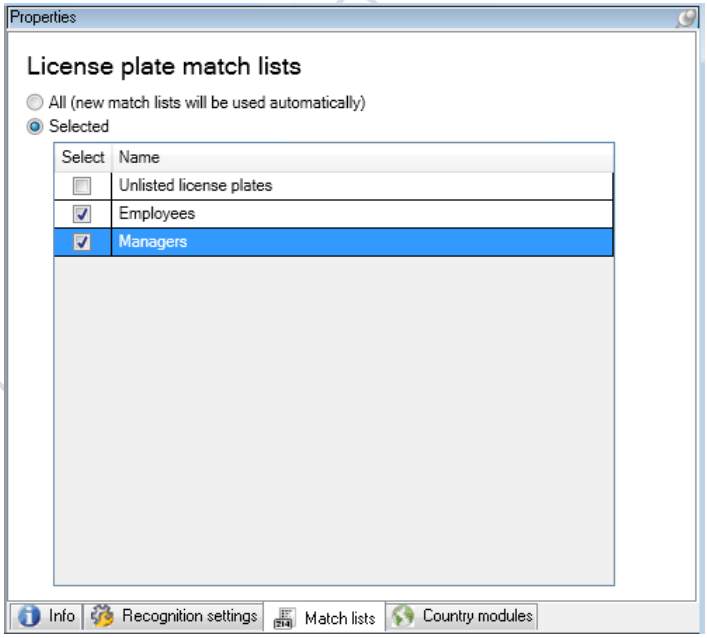
Nombre	Descripción
Compensar entrelazado	Si su cámara LPR graba vídeo entrelazado y ve un efecto de peinado en la imagen desentrelazada en LPR, seleccione esta casilla de verificación. Esto puede mejorar la calidad de la imagen y los resultados de reconocimiento.
Número máximo de fotogramas por segundo procesado	Limite el número de fotogramas que su sistema procesa cada segundo. Si mantiene esta configuración baja, puede aumentar la velocidad de fotogramas en su cámara sin agregar carga innecesaria a su servidor LPR. **Ilimitado:** Quite el límite superior. Usted correrá el riesgo de aumentar el tiempo de procesamiento y la carga de la CPU.
Número máximo de segundos utilizado por trama	Limite el número de segundos que su LPR puede gastar para reconocer un fotograma. Si se ajusta, el valor recomendado es de 0,2 segundos por fotograma. **Ilimitado:** Quite el límite superior. Usted correrá el riesgo de aumentar el tiempo de procesamiento y la carga de la CPU.
Detener el reconocimiento anterior	Detenga el reconocimiento cuando se reconozca una placa de licencia con un nivel de confianza igual o superior al valor que especifique.

Nombre	Descripción
Descarte los reconocimientos a continuación	Deseche los reconocimientos con un nivel de confianza por debajo del valor que especifique. Aumente este valor para obtener menos, pero posiblemente, reconocimientos más precisos. Disminuir este valor para obtener más, pero potencialmente menos reconocimientos precisos. Cuanto menor sea la diferencia entre **Detener el reconocimiento por encima de** y **Descartar reconocimientos por debajo de** valores, menor será el tiempo de procesamiento y la carga de CPU.
El número máximo de placas de matrícula reconocido por trama	Reconocer varias placas simultáneamente. Por ejemplo, es relevante para cámaras que registran caminos de múltiples carriles, donde muchas placas deben ser reconocidas al mismo tiempo. **Ilimitado:** Quite el límite superior. Usted correrá el riesgo de aumentar el tiempo de procesamiento y la carga de la CPU.
Tiempo en segundos para evitar los reconocimientos parciales	Retrasar todos los reconocimientos para el período de tiempo especificado. Esto es para evitar que la misma placa sea reconocida varias veces como placas de licencia diferentes. El sistema esperará un mejor reconocimiento y sólo aceptará el reconocimiento más completo. Nota: Antes de cambiar este ajuste, asegúrese de que ningún objeto móvil no relevante (ver "Angulos de camara" en la página *342*) bloquee la vista de su cámara LPR.

Después de cambiar la configuración de su cámara LPR, validar su configuración (ver "Validar configuración" en la página 365) para comprobar si el sistema reconoce placas de la licencia, así como se espera.

Pestaña Lista de coincidencias

En esta pestaña se selecciona la lista de coincidencias de matrículas que desea que una cámara LPR específica coincida con las matrículas. Puede crear tantas listas como usted necesita (ver "Añadir nuevas listas de coincidencia de matrículas" en la página 366).



Nombre	Descripción
Todo	Las placas de matrícula se comparan con todas las listas disponibles y futuras.
Seleccionado	Las placas de matrícula se comparan con sólo las listas seleccionadas. Seleccionar una o más de las listas disponibles.

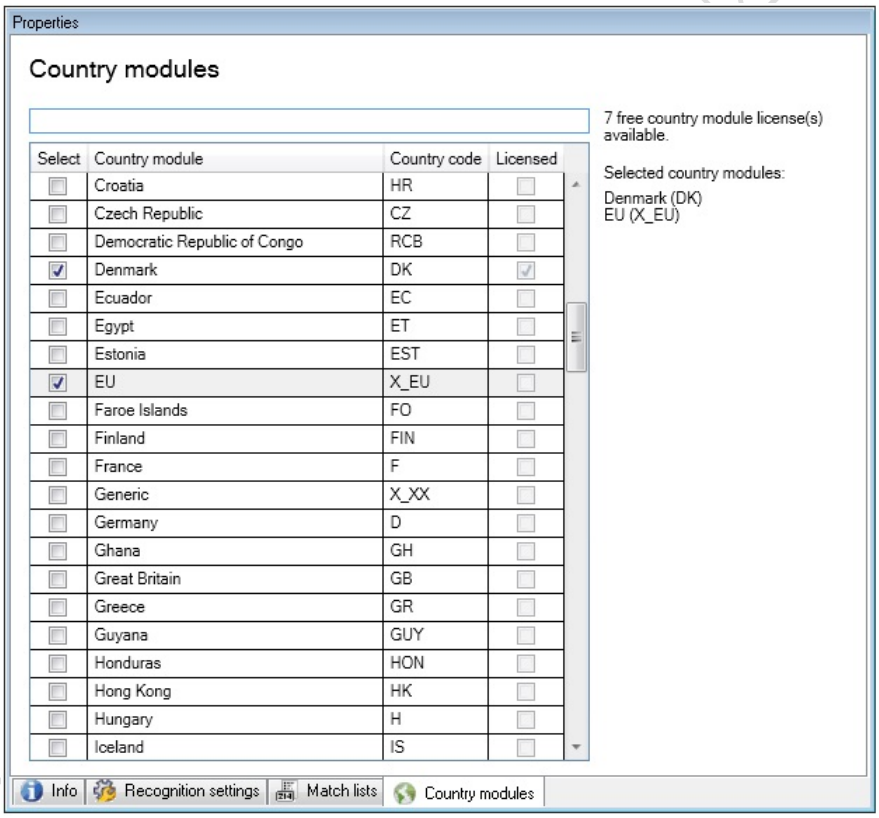
Después de cambiar la configuración de su cámara LPR, validar su configuración (ver "Validar configuración" en la página 365) para comprobar si el sistema reconoce placas de la licencia, así como se espera.

Pestaña modulos país

Aquí puede seleccionar los módulos de país que desea utilizar con una cámara LPR específica. La lista que se puede elegir, depende de los módulos que haya instalado y sus licencias (ver "Licencias XProtect LPR" en la página 339).

Un módulo país es un conjunto de reglas que define placas de matrícula de un cierto tipo y forma de pertenecer a un país determinado, estado o región.

Los módulos ya licenciados aparecen con una marca de verificación en la columna **Con licencia**. Si el módulo país que busca no está en la lista, póngase en contacto con su proveedor.



Nombre	Descripción
Seleccionar	Haga clic para seleccionar o anular la selección de un módulo país. La lista de los módulos de los países seleccionados en el lado derecho se actualiza automáticamente.

Nombre	Descripción
Módulo país	Lista los módulos instalados país.
Código de país	Las letras que identifican un módulo país.
Con licencia	Muestra si un módulo país ya tiene licencia. Puede seleccionar un módulo rural autorizada para tantas cámaras como desee.

Después de cambiar la configuración de su cámara LPR, validar su configuración (ver "Validar configuración" en la página 365) para comprobar si el sistema reconoce placas de la licencia, así como se espera.

Prolongar el tiempo para evitar reconocimientos parciales

Si se reconocen partes de la misma placa como números de placas independientes e incompletos, asegúrese de que ningún objeto móvil no relevante (ver "Angulos de camara" en la página 342) bloquee la vista de su cámara LPR. Si el problema persiste, dé al sistema más tiempo para evitar reconocimientos parciales. Tus reconocimientos serán más precisos, pero todos aparecerán retrasados.

1. En el panel **Panel Navegación del sitio** , expanda **Servidores.**
2. Expandir **LPR servidores** y haga clic en **LPR**cámaras.
3. En el panel **LPR** , busque y haga clic en la cámara para modificarla.
4. En la **Configuración de reconocimiento** ficha, haga clic en **Configuración avanzada**.
5. En el campo **Tiempo de espera para evitar los reconocimientos parciales** , arrastre el control deslizante a la derecha para dar al sistema un máximo de cinco segundos adicionales para reconocer los números de matrícula más completos y descartar el resto.

Seleccionar instantáneas

Cuando configuró el LPR inicialmente con el **Añadir cámara LPR** asistente, también agregó instantáneas (ver "Instantáneas (explicadas)" en la página 355). Siempre se puede añadir instantáneas representativas adicionales para mejorar la optimización de la configuración.

1. Seleccione la cámara correspondiente.
2. En la pestaña **programación de reconocimiento**, haga clic **Instantáneas**.
3. Capturar instantáneas de vídeo en directo o importarlos desde una ubicación externa. Haga clic en **Siguiente**.

   El sistema analiza las instantáneas que ha seleccionado para la cámara.
4. En la página siguiente, aprobar o rechazar cada una de las instantáneas. Si el sistema no puede reconocer placas de cualquier licencia, haga clic en **Anterior** para añadir nuevas instantáneas en una mejor calidad. Si el sistema todavía no puede proporcionar reconocimientos correctos, es probable que tenga que cambiar su configuración. Compruebe que la cámara esté montada y configurada correctamente (ver "Preparación de cámaras para LPR (explicado)" en la página 340).
5. Una vez que haya aprobado todas las instantáneas, haga clic en **Siguiente** y cerrar el asistente.
6. En la ficha **Ajustes Reconocimiento**, haga clic **Validar configuración** (en la página 365).

Validar configuración

Puede validar la configuración actual para ver si necesita cambiar ninguna configuración o proporcionar más instantáneas. La función de validación le informa sobre el número de placas de licencias reconoce el sistema, y si se reconoce correctamente.

Puede ayudar a decidir si su nivel de confianza se establece correctamente y si la configuración del sistema es óptima.

1. Seleccione la cámara correspondiente.
2. Desde la pestaña **reconocimiento ajustes**, haga clic en **Validar configuración**.

   Sobre la base de la configuración actual, el sistema analiza las instantáneas que ha seleccionado para la cámara y ofrece un resumen de los resultados:

   - **Placas detectadas:** El número de matrículas reconocidas, por ejemplo, 3 de 3.
   - **Confiabilidad media:** El porcentaje promedio de confianza con la que se han reconocido las placas de matrícula.
   - **Tiempo medio de procesamiento**; El promedio de tiempo que se tardó en analizar una instantánea y volver una lectura medido en ms.

License plates detected:	**2 of 2**
Average confidence:	**91 %**
Average processing time:	**112 ms**

3. Si la configuración actual se adapte a sus necesidades, haga clic en **Cerrar**.
4. Si desea investigar más los resultados, haga clic en **Siguiente** y puede revisar los resultados de cada instantánea. Esto le ayuda a identificar las situaciones que causan problemas.

Puede validar la configuración tantas veces como desee y en cualquier cámara LPR y con diferentes configuraciones.

Configuración automática

La configuración automática de la cámara LPR sobrescribe los cambios manuales realizados en los ajustes. Puede seleccionar esta opción si, por ejemplo, se han realizado cambios manuales que no le han dado buenos resultados del reconocimiento.

1. Desde el reconocimiento **ajustes** pestaña, haga clic en c**onfiguración automática**.

   Aparece un nuevo cuadro de diálogo.
2. Confirmar que desea volver a los ajustes configurados automáticamente haciendo clic en **Siguiente**.

   El sistema optimiza la configuración.
3. Haga clic en **Cerrar**.
4. Si se le solicita, confirme para guardar la configuración.
5. Revisar y validar (ver "Validar configuración" en la página 365) la nueva configuración.

Trabajar con listas de coincidencia de matrículas

Listas de matrículas (explicadas)

Las listas de matrículas son colecciones de matrículas que desea que su solución LPR trate de manera especial. Los reconocimientos de matrículas se comparan con estas listas y si hay una coincidencia, el sistema activa un evento LPR. Los eventos se almacenan en el servidor de eventos y se pueden buscar y ver en la ficha **LPR** en XProtect Smart Client.

De forma predeterminada, los eventos se almacenan durante 24 horas. Para cambiar esto, abra el cuadro de diálogo **Opciones** en el Management Client y en la pestaña **Configuración del servidor eventos** en el campo **conservar eventos pare**, ingrese un nuevo marco de tiempo.

Después de especificar una lista de coincidencias de matrículas, puede configurar eventos y alarmas adicionales que se activarán en una coincidencia.

Ejemplos:

- Una sede de la empresa utiliza una lista de placas de automóviles compañía de gestión ejecutiva de conceder el acceso a los ejecutivos de una zona de aparcamiento independiente. Cuando se reconocen las placas de matrícula de los ejecutivos, la solución LPR activa una señal de salida que abre la compuerta al área de estacionamiento.
- Una cadena de estaciones de servicio crea una lista de las matrículas de los vehículos que han dejado previamente estaciones de servicio sin pagar por su gas. Cuando se reconocen tales placas, LPR activa señales de salida que activan una alarma y bloquean temporalmente el suministro de gas a ciertas bombas de gas.

Eventos activados también se pueden utilizar para la fabricación de cámaras graban en alta calidad o similar. Incluso puede utilizar un evento para activar combinaciones de tales acciones.

Lista de matrículas no listadas (explicada)

Frecuencia con la que disparar un evento cuando se reconoce una placa de matrícula que se incluye en una lista, pero también se puede desencadenar un evento con una placa de matrícula, que es **no** incluido en una lista.

Ejemplo: Hay un aparcamiento privado utiliza una lista de placas de matrícula para conceder los vehículos de los residentes el acceso al aparcamiento. Si un vehículo con una matrícula que no está en la lista se acerca al aparcamiento, la solución LPR dispara una señal de salida que enciende un cartel que indica al conductor que obtenga un pase de invitado temporal de la oficina de seguridad.

Para activar un evento del sistema de vigilancia, cuando se reconoce una placa de matrícula **no** en una lista, use la **Lista de matrículas no listadas**. Lo selecciona para una cámara como cualquier otra lista (ver "Pestaña Lista de coincidencias" en la página 362) y configurarlo como cualquier otra lista (ver "Eventos desencadenados por LPR " en la página 369).

Añadir nuevas listas de coincidencia de matrículas

1. En el **Panel Navegación del sitio**, seleccione **Lista de coincidencias de matrículas**, haga clic con el botón secundario del mouse y seleccione **Añadir nuevo**.
2. En la ventana que aparece, de la lista un nombre y haga clic en **OK**.

   Tan pronto como haya creado una lista de placas de matrícula, se hace visible en la **Lista de matrículas de matrícula** y en el **Lista de coincidencias** ficha para todas las cámaras LPR.

3. Si desea añadir columnas a la lista de coincidencias, haga clic **campo personalizado** y especificar las columnas en el cuadro de diálogo que se abre (ver "Editar campos personalizados propiedades" en la página 369).
4. Para actualizar la lista de coincidencias, utilice botones (ver "Edición de listas de matrículas coincidentes" en la página 367) **Añadir**, **Editar**, **Borrar**.
5. En lugar de definir la lista de coincidencias directamente en el Management Client, puede importar un archivo (ver "Importación/exportación de listas de matrículas coincidentes" en la página 367).
6. Si se le solicita, confirme el guardar los cambios.

Edición de listas de matrículas coincidentes

1. En el **Panel Navegación del sitio**, seleccione **Lista de coincidencias de matrículas**.
2. Ir al panel general. Haga clic en la lista correspondiente.
3. La**lista de coincidencia de matrículasinformación** abre la ventana.
4. Para incluir nuevas filas a la lista, haga clic en **Añadir** y rellene los campos siguientes:
   - No incluya ningún espacio.
   - Siempre utilice mayúsculas.

     Ejemplos: ABC123 (correcto), ABC 123 (incorrecto), abc123 (incorrecto)
   - Puede utilizar comodines en las listas de coincidencia de matrículas. Para ello, la definición de las placas con una serie de? y la letra(s) y / o número(s) que debe aparecer en lugares específicos.

     Ejemplos:?????A, A?????, ???1??, 22??33, A?B?C?o similares.
5. Si se le solicita, confirme el guardar los cambios.

Importación/exportación de listas de matrículas coincidentes

Puede importar un archivo con una lista de placas de matrícula que desea utilizar en una lista de coincidencias de matrículas. Dispone de las siguientes opciones de importación:

- Añadir matrículas a la lista existente.
- Sustituir la lista existente.

Esto es útil si, por ejemplo, las listas se gestionan desde una ubicación central. A continuación, todas las instalaciones locales se pueden actualizar mediante la distribución de un archivo.

Del mismo modo, puede exportar la lista completa de placas de matrícula a partir de una lista de coincidencias a una ubicación externa.

Formatos de archivo admitidos son . txt o . csv.

Para importar, proceda del siguiente modo:

1. En **Panel Navegación del sitio**, haga clic en **Lista de coincidencias de matrículas** y seleccione la lista correspondiente.
2. Para importar un archivo, haga clic en **Importar**.

3. En el cuadro de diálogo, especifique la ubicación del archivo de importación y el tipo de importación. Haga clic en **Siguiente**.
4. Espere hasta recibir la confirmación y haga clic en **Cerrar**.

Para exportar, proceda del siguiente modo:

1. Para exportar un archivo, haga clic en **Exportar**.
2. En el cuadro de diálogo, especifique la ubicación del archivo de exportación y haga clic en **Siguiente**.
3. Haga clic en **Cerrar**.
4. Puede abrir y editar el archivo exportado en, por ejemplo, Microsoft Excel.

Propiedades de listas de coincidencia de matrículas

Nombre	Descripción
Nombre	Muestra el nombre de la lista. Si es necesario, puede cambiar el nombre.
Campos Personalizados	Haga clic para especificar las columnas de entrada que la matrícula que usted o el usuario del cliente puede añadir información adicional a. Ver campos personalizados (propiedades) (ver "Editar campos personalizados propiedades" en la página 369).
Buscar	Buscar en la lista de placas de matrícula, números específicos, patrones o similares. Si es necesario, puede utilizar ? como un solo comodín
Añadir	Haga clic para añadir una placa de matrícula. • No incluya ningún espacio. • Siempre utilice mayúsculas. **Ejemplos:** ABC123 (correcto), ABC 123 (incorrecto), abc123 (incorrecto) • Puede utilizar comodines en sus listas de placas de matrícula. Para ello, la definición de las placas con una serie de? y la(s) letra(s) y / o número(s) que debe aparecer en lugares específicos. **Ejemplos:**?????A, A?????, ???1??, 22??33, A?B?C? y similares. Algunas áreas regionales pueden tener excepciones a estas reglas. Por ejemplo, las placas personalizado con espacios. Placas con dos conjuntos de caracteres que deben ser reconocidos por separado por un carácter de subrayado (). O placas de ciertas regiones con letras en un color de fondo diferente en partes de la placa de matrícula. **Ejemplo:** 
Editar	Haga clic para editar una placa de matrícula. Se pueden seleccionar varias filas para la edición.
Borrar	Haga clic para eliminar la placa de licencia seleccionada (s).

Nombre	Descripción
Importar	Haga clic para importar placas de matrícula de cualquier archivo separado por comas, por ejemplo, un archivo . txt- o CSV-archivo (ver "Importación/exportación de listas de matrículas coincidentes" en la página 367).
Exportación	Haga clic para exportar el listado de matrículas en un archivo separado por comas, por ejemplo, un archivo . txt- o CSV-archivo (ver "Importación/exportación de listas de matrículas coincidentes" en la página 367).
Filas por página	Seleccionar el número de placas de matrícula para mostrar en una página (una pantalla). Se puede elegir entre 50 a 1000 filas.
Eventos activados por partido de la lista	Seleccione qué evento(s) debe ser activado por un coincidencia de lista (ver "Eventos desencadenados por LPR " en la página 369). Se puede elegir entre todos los tipos disponibles de eventos definidos en el sistema.

Editar campos personalizados propiedades

Puede añadir columnas a las listas de coincidencia de matrículas para obtener información adicional. Se define el nombre y el número de columnas, así como el contenido del campo.

Los usuarios de XProtect Smart Client pueden actualizar la información de las columnas, pero no las propias columnas.

Nombre	Descripción
Añadir	Añade una columna a la lista de coincidencias. Escriba un nombre para la columna.
Editar	Haga clic para editar el nombre de la columna.
Borrar	Elimina una columna.
Arriba	Cambia el orden de las columnas.
Abajo	Cambia el orden de las columnas.

Eventos desencadenados por LPR

Después de tener lista de coincidencia de matrículas creado (ver "Añadir nuevas listas de coincidencia de matrículas" en la página 366), puede asociarlos con todos los tipos de eventos definidos en el sistema.

El tipo de eventos disponibles depende de la configuración de su sistema. En conexión con LPR, los eventos se utilizan para activar señales de salida para, por ejemplo, elevar la barrera de aparcamiento o hacer que las cámaras sean de alta calidad. También puede utilizar un evento para activar combinaciones de tales acciones. Ver Listas de matrículas (explicado) (ver "Listas de matrículas (explicadas)" en la página 366) para más ejemplos.

Configurar eventos del sistema provocados por coincidencias de la lista

1. Expandir **Servidores**, haga clic **lista de coincidencia de matrículas** y seleccione la lista a la que desea asociar un evento.
2. En ventana **Información de lista de coincidencia de matrículas**, junto a campo de selección **Eventos activados por el campo de lista de coincidencias**, haga clic en **Seleccionar**.
3. En el **Seleccionar desencadena eventos** cuadro de diálogo, seleccione uno o más eventos.
4. Si se le solicita, confirme el guardar los cambios.
5. El evento se asocia ahora con reconocimientos en la lista de coincidencias de matrículas seleccionado.

Para desencadenar un evento del sistema de vigilancia, cuando una matrícula que es **no** en una lista se reconoce, configurar las placas de lista **matrícula sin cotización**.

Alarmas activadas por LPR

Puede asociar algunos tipos de alarmas con eventos de XProtect LPR. Proceda del siguiente modo:

1. Crear la lista de coincidencias de matrículas (ver "Añadir nuevas listas de coincidencia de matrículas" en la página 366) desea hacer coincidir las matrículas en contra.
2. Agrega y configura tu (s) cámara (es) LPR . (ver "Añadir cámara LPR" en la página 356)
3. En el **Panel Navegación del sitio**, expanda **Alarmas**, haga clic con el botón secundario en **Definiciones de alarma** y seleccione para crear una nueva alarma.
4. Aparecerá la ventana **Información de definiciones de alarma**. Seleccione las propiedades (ver "Definiciones de alarma para LPR" en la página 370) relevantes.
5. Si se le indica cuando está hecho, confirmar para guardar los cambios.
6. Configure los ajustes de datos de alarma para LPR . (ver "Configuración de datos de alarma para LPR" en la página 371)

Definiciones de alarma para LPR

Excepto para definir **Eventos de disparo**, los ajustes para **Las definiciones de alarma** son las mismas para LPR que para la parte restante del sistema.

Para definir eventos de disparo relacionados con LPR, seleccione el mensaje de evento que se utilizará cuando se active la alarma:

1. En el campo **Activación de eventos**, en la lista desplegable superior, decida qué tipo de evento utilizar para la alarma. La lista ofrece **Listas de matrícula** y eventos (ver "Trabajar con listas de coincidencia de matrículas" en la página 366) **LPR servidor**.
2. En la segunda lista desplegable, seleccione el mensaje de evento específico para utilizarlo. Si seleccionó **Lista de coincidencias de matrículas** en el menú desplegable anterior, seleccione una lista de matrículas. Si seleccionó **servidor LPR**, seleccione el mensaje de evento de servidor LPR correspondiente:
   - Se pierde la conexión de la cámara LPR
   - LPR cámara en funcionamiento
   - El servidor LPR no responde

- Respuesta del servidor LPR

Para obtener información acerca de los ajustes de alarma restantes definición, ver las **alarmas** sección.

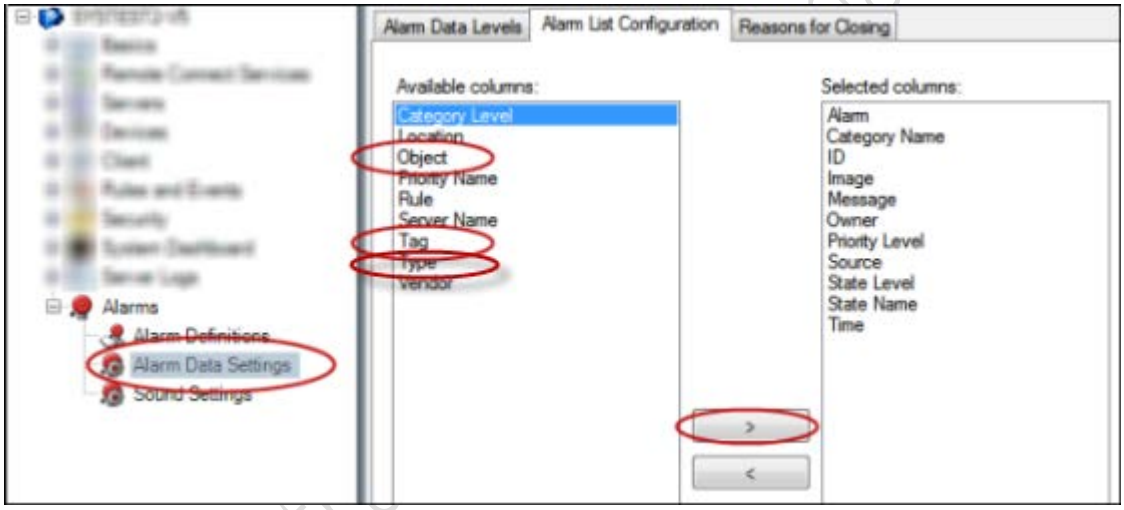
Configuración de datos de alarma para LPR

En Management Client, debe crear dos elementos **de configuración de lista de alarmas** disponibles para su selección en XProtect Smart Client.

Estos dos elementos se utilizan para configurar las listas de alarmas en la pestaña **Gestor de alarma** en XProtect Smart Client. Los elementos relevantes son **Objeto**, **etiqueta** y **tipo**, que son esencial para reconocer números de matrícula (objeto) y códigos de país (etiqueta).

Haga lo siguiente en el Management Client:

1. En el **Panel Navegación del sitio**, expanda **Alarms**, seleccione **Configuración de datos de alarma**.
2. En pestaña **Lista de configuración alarma**, seleccione **Objeto**, **Tag** , y **Tipo** y haga clic **>** .



3. Si se le solicita, confirme el guardar los cambios.

Mantenimiento LPR

Acerca de LPR Server Manager

Cuando haya instalado un servidor LPR, puede comprobar el estado de sus servicios con XProtect LPR Server Manager. Puede, por ejemplo, iniciar y detener el servicio de servidor de <LPR>, mensajes de estado de vista, y leer los archivos de registro.

- Puede acceder a la información de estado del servidor LPR mediante el icono LPR Server Manager en el área de notificación del equipo **que ejecuta el servidor LPR**.

En el Management Client, puede obtener una descripción completa del estado de todos sus servidores LPR (ver "Ver información del servidor LPR" en la página 353).

Iniciar y detener el servicio del servidor LPR

El servicio del servidor LPR se inicia automáticamente después de la instalación. Si ha dejado el servicio manualmente, puede reiniciar manualmente.

1. Haga clic con el botón secundario en el icono LPR Server Manager en el área de notificación.
2. En el menú que aparece, seleccione **Inicie el servicio de servidor LPR**.
3. Si es necesario, seleccione **Detener servicio del servidor LPR** para detener el servicio de nuevo.

Mostrar estado del servidor LPR

1. En el servidor LPR, haga clic con el botón derecho en el icono LPR Server Manager en el área de notificación.
2. En el menú que aparece, seleccione **Mostrar estado del servidor LPR**.

   Si el sistema está funcionando sin problemas, la situación es la siguiente: Todas las cámaras LPR funcionando.

   Otros estados son:

   - El servicio no está respondiendo
   - No está conectado al sistema de vigilancia
   - El servicio no está funcionando
   - Servidor de eventos no está conectado
   - Error desconocido
   - X de Y LPR cámaras funcionando

Mostrar registro del servidor LPR

Los archivos de registro son una herramienta útil para supervisar y solucionar el estado del servicio LPR Server. Todas las entradas son con fecha y hora, con las entradas más recientes en la parte inferior.

1. En el área de notificación, haga clic con el botón secundario en icono Administrador servidor LPR.
2. En el menú que aparece, seleccione **Mostrar el archivo de registro del servidor LPR**.

   Un registro-visor muestra las actividades del servidor con marcas de tiempo.

Cambiar la configuración del servidor LPR

El servidor LPR debe poder comunicarse con su servidor de administración. Para habilitarlo, especifique la dirección IP o el nombre de host del servidor de administración durante la instalación del servidor LPR.

Si es necesario cambiar la dirección del servidor de gestión, haga lo siguiente:

1. Detener (ver "Iniciar y detener el servicio del servidor LPR" en la página 372) el servicio LPR Server.
2. En el área de notificación, haga clic con el botón secundario en icono Administrador servidor LPR.
3. En el menú que aparece, seleccione **Cambiar la configuración**. Aparecerá la ventana **LPR Server service**.

4. Especificar los nuevos valores y haga clic en **OK**.
5. Reinicie el servicio LPR Server.

Desinstalación XProtect LPR

Si desea quitar XProtect LPR de su sistema, desinstalar los dos componentes por separado utilizando el procedimiento de extracción normal de Windows:

- En los equipos donde está instalado el complemento XProtect LPR , desinstale Milestone XProtect LPR [versión] Plug-in.
- En los equipos donde está instalado el servidor de XProtect LPR, desinstalar Milestone XProtect LPR Servidor [versión].

XProtect Transact

XProtect Transact introducción

XProtect Transact (explicado)

Funcionalidad disponible depende del sistema que está utilizando. Ver la tabla de comparación de productos para obtener más información.

XProtect Transact es un complemento de las soluciones de videovigilancia IP de Milestone.

XProtect Transact es una herramienta para observar transacciones en curso e investigar transacciones en el pasado. Las transacciones están vinculadas con el vídeo digital de vigilancia el seguimiento de las transacciones, por ejemplo, para ayudar a probar fraude o se evidencia en contra de un agresor. Hay una relación de 1 a 1 entre las líneas de transacción e imágenes de vídeo.

Los datos de la transacción se pueden originar en diferentes fuentes de transacción, normalmente sistemas de puntos de venta (PoS) o máquinas de extracción automatizadas (ATM).

Arquitectura del sistema XProtect Transact

Hay varios componentes en el flujo de comunicación XProtect Transact. Los datos de entrada se origina en las cámaras de vigilancia de vídeo y las fuentes de transacción que proporcionan los datos de las transacciones, por ejemplo cajas registradoras o cajeros automáticos. Los datos de transacción se almacenan en el servidor de eventos, mientras que el flujo de vídeo se almacena en el servidor de grabación. A partir de los servidores, los datos se pasan a XProtect Smart Client.

Dependiendo de su sistema, puede haber varios servidores de grabación.

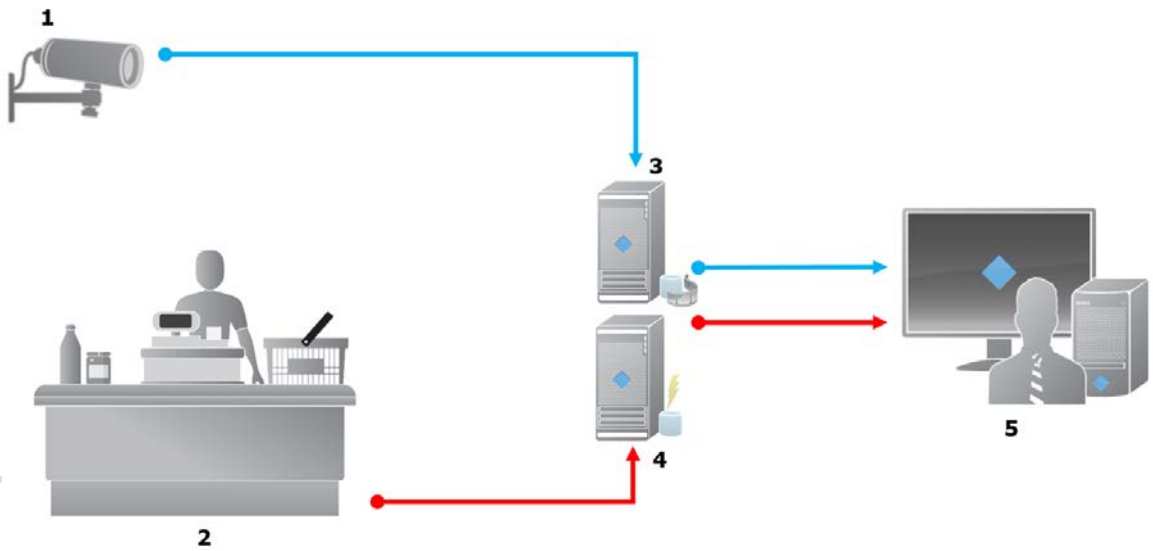


Ilustración:

- 1 = la cámara.
- 2 = registro efectivo.

- 3 = El servidor de grabación.
- 4 = servidor de eventos.
- 5 = Cliente Inteligente.
- Las flechas azules describen grabaciones de vídeo desde el sistema de vigilancia.
- Las flechas rojas de esquema de datos de transacción de las fuentes de transacción.

Por estándar, XProtect Transact admite dos tipos de fuentes de transacción:

- Clientes del puerto serie.
- Clientes del servidor TCP.

Otros tipos de fuentes de transacción pueden ser apoyados a través de conectores personalizados desarrollados con el kit de desarrollo de software MIP (SDK), por ejemplo, un conector que recupera los datos de transacciones de un sistema de planificación de recursos empresariales (ERP).

Conectores (explicados)

Un conector facilita la importación de datos de transacción sin procesar desde la fuente de transacción, por ejemplo el ATM, al servidor de eventos asociado con el VMS.

Los conectores integrados disponibles se describen en la tabla:

Nombre	Descripción
Conector de cliente TCP	Utilizar cuando el origen de la transacción proporciona los datos de la transacción a través de una interfaz de servidor TCP. Este conector tiene dos valores que se pueden especificar: nombre de host y el número de puerto.
Conector de puerto serie	Utilizar cuando se reciben datos de transacción como entrada en un puerto serie en el servidor de eventos.

Conectores desarrollados a través del kit de desarrollo de software MIP también pueden estar disponibles.

Ver también

Añadir origen de la transacción (asistente) (en la página 377)

Definiciones de transacciones (explicadas)

Una definición transacción es un grupo de valores que ayudan a controlar cómo se muestran los datos en bruto de las fuentes de transacción en el XProtect Smart Client junto con las grabaciones de vídeo. La salida es un formato de fácil lectura que se asemeja a los recibos de la vida real, por ejemplo recibos de caja y los recibos de los cajeros automáticos.

Más específicamente, las definiciones de transacción le permiten:

- definir cuándo las transacciones individuales comienzan y terminan.
- insertar saltos de línea según sea necesario.
- filtrar los caracteres no deseados o cadenas de texto, por ejemplo, si los datos proceden de una conexión de impresora y contiene caracteres no imprimibles para indicar los saltos de línea, cuando para cortar un recibo de caja.

- caracteres de sustitución con otros personajes.

Puede utilizar la misma definición de transacciones en múltiples fuentes de transacción.

Ver también

Añadir transacción definiciones (en la página 379)

Eventos de transacción (explicados)

Un evento de transacción es la aparición de determinadas palabras, números o caracteres en el flujo de datos de la transacción que fluye de las fuentes de transacciones, por ejemplo, las cajas registradoras, al servidor de eventos. Como administrador del sistema, es necesario definir lo que son los eventos. Esto permite al operador para realizar un seguimiento e investigar los eventos de transacción en XProtect Smart Client. Para cada evento, un método (tipo de concordancia) debe especificarse para identificar las cadenas en los datos de transacción: coincidencia exacta, comodín o expresiones regulares.

Ver también

Definir un evento de transacción (ver "Definir eventos de transacción" en la página 382)

Crear una alarma de transacción (ver "Cree alarmas basadas en eventos de transacciones" en la página 383)

Compatibilidad

XProtect Transact es compatible con la versión 2016 R1 o posterior de:

- XProtect Corporate
- XProtect Expert

XProtect Transact es compatible con la versión 2017 R2 o posterior de:

- XProtect Professional+
- XProtect Express+

Primeros pasos

La funcionalidad XProtect Transact es estándar en Management Client. Cuando haya activado las licencias de licencia base y origen de la transacción, las funciones están disponibles inmediatamente. Antes de utilizar las funciones XProtect Transact en XProtect Smart Client, debe:

1. Compruebe que se ha activado su licencia base para XProtect Transact. Además, compruebe que tiene una licencia de código de transacción para cada fuente de transacción necesaria para supervisar. Información de licencia está disponible en el nodo **Basics**.

   Si usted no tiene el número suficiente de licencias de código de transacción, asegúrese de que adquiere licencias adicionales antes de que expire el período de gracia -days 30.

2. Añadir y configurar las fuentes que proporcionan los datos de la transacción, por ejemplo, las cajas registradoras. Para obtener más información, consulte Añadir fuente de transacción (asistente) (ver "Añadir origen de la transacción (asistente)" en la página 377).

3. (Opcional) Definir los eventos de transacciones y potencialmente configurarlos para desencadenar reglas o alarmas. En XProtect Smart Client, el operador puede investigar los eventos de transacciones.

Aunque no haya adquirido ninguna licencia XProtect Transact, puede probar XProtect Transact con una licencia de prueba. Para obtener más información, consulte Licencia de prueba de XProtect Transact (en la página 377).

Ver también

Configuración de transacciones (en la página 377)

La creación de eventos (ver "Configuración de eventos de transacciones y alarmas" en la página 382)

Licencia de prueba de XProtect Transact

Con una licencia de prueba de XProtect Transact puede usar las funcionalidades de XProtect Transact durante 30 días. Todas las funciones relacionadas están activadas, y puede añadir una fuente de transacción, como una máquina registradora. Cuando concluye el periodo de prueba de 30 días, todas las funciones de XProtect Transact se desactivan, incluyendo el espacio de trabajo **Transacción** y los elementos de la vista de transacción. Al comprar y activar una licencia básica de XProtect Transact y la licencias de fuentes de transacción necesarias, puede usar XProtect Transact de nuevo y se conservarán los ajustes y datos.

Si está usando productos de XProtect Professional VMS, la licencia de prueba está integrada. La licencia de prueba se activa cuando el administrador del sistema añade una fuente de transacción a la configuración.

En el caso de otros productos, tiene que adquirir la licencia de prueba de Milestone. El administrador del sistema debe activar la licencia de prueba en la configuración.

XProtect Transact configuración

Configuración de transacciones

En esta sección, aprenderá cómo añadir y configurar las fuentes de transacción, y cómo crear las definiciones de transacción.

Añadir origen de la transacción (asistente)

Para conectar datos de una fuente de transacción a XProtect Transact, debe añadir los orígenes de las transacciones, por ejemplo un cajero automático. En el asistente, se selecciona un conector, y se puede conectar una o más cámaras.

Si usted no tiene una licencia de código de transacción para el origen de la transacción que está a punto de añadir, el sistema funcionará durante el período de gracia 30 -days. Asegúrese de que usted adquiere una licencia de código de transacción adicionales y que se active a su debido tiempo.

Pasos:

1. En el **Panel Navegación del sitio**, expanda **Transact**.
2. Ir al panel general. Haga clic con el botón secundario en el nodo **Origen de las transacciones** y seleccione **Añadir fuente**. Aparece el asistente.
3. Siga los pasos del asistente.
4. Dependiendo del conector selecciona, aparecen diferentes campos que tiene que rellenar. Para obtener más información, consulte Fuentes de transacción (propiedades) (en la página 378). Puede cambiar esta configuración después de completar el asistente.

5. Si la definición de transacción que usted necesita no está disponible, haga clic en **Añadir nuevo** para crear una nueva definición de transacción.

Ver también

Añadir transacción definiciones (en la página 379)

Conectores (explicados) (en la página 375)

Fuentes de transacción (propiedades)

Los ajustes para las fuentes de transacción se describen en la tabla.

Nombre	Descripción
Habilitar	Si desea desactivar el origen de la transacción, desactive esta casilla de verificación. El flujo de datos de la transacción se detiene, pero los datos ya importados se mantienen en el servidor de eventos. Aún se pueden ver las transacciones desde una fuente de transacciones con discapacidad en XProtect Smart Client durante su período de conservación. Incluso una fuente de transacciones con discapacidad requiere una licencia de código de transacción.
Nombre	Si desea cambiar el nombre, introduzca un nuevo nombre aquí.
Conector	No se puede cambiar el conector que seleccionó al crear el origen de la transacción. Para seleccionar un conector diferente, es necesario crear un nuevo origen de la transacción, y durante el asistente, seleccione el conector que desee.
Definición de transacción	Se puede seleccionar una definición diferente de transacción que define cómo transformar los datos de las transacciones recibidas en las transacciones y líneas de transacción. Esto incluye la definición: • cuando una transacción comienza y termina. • cómo las transacciones se muestran en XProtect Smart Client.
Periodo de retención	Especificar, en días, de cómo los datos de transacciones de largo se mantienen en el servidor de eventos. El período de retención predeterminado es de 30 días. Cuando expira el período de retención, se elimina automáticamente los datos. Esto es para evitar la situación, cuando se rebase la capacidad de almacenamiento de la base de datos. El valor mínimo es 1 día, mientras que el valor máximo es de 1000 días.
Conector de cliente TCP	Si ha seleccionado **conector de cliente TCP**, especificar estos valores: • **Nombre de host**: introduzca el nombre de host del servidor TCP asociado con el origen de la transacción. • **Puerto**: introduzca el nombre del puerto en el servidor TCP asociado con el origen de la transacción.

Nombre	Descripción
Conector de puerto serie	Si ha seleccionado **conector de puerto serie**, especificar estos parámetros y asegúrese de que coinciden con la configuración de la fuente de transacción: • **Puerto serie**: seleccione el puerto COM. • **Velocidad en baudios**: especifique el número de bits transmitidos por segundo. • **Paridad**: especifique el método para detectar errores en las transmisiones. De forma predeterminada, se selecciona **Ninguno**. • **Bits de datos**: especifica el número de bits utilizados para representar un carácter de datos. • **Detener bits**: especifica el número de bits para indicar cuándo se ha transmitido un byte. La mayoría de los dispositivos necesitan de 1 bit. • **Del apretón de manos**: especificar el método de establecimiento de determinar el protocolo de comunicación entre el origen de la transacción y el servidor de eventos.

Ver también

Añadir origen de la transacción (asistente) (en la página 377)

Añadir transacción definiciones (en la página 379)

Añadir transacción definiciones

Como parte de la definición de un origen de la transacción, se especifica una definición de la fuente. Una definición transforma los datos en bruto recibidos en datos presentables, de modo que los usuarios puedan ver los datos de XProtect Smart Client en un formato que coincida con los recibos de la vida real. Esto es necesario, ya que normalmente los datos en bruto constan de una sola cadena de datos, y puede ser difícil de ver en las transacciones individuales comienzan y terminan.

Pasos:

1. En el **Panel Navegación del sitio**, expanda **Transact**.
2. Seleccione **Transacción definiciones**.
3. Ir al panel general. Haga clic con el botón derecho en **Definición de transacción** y seleccione **Añadir nuevo**. Una serie de ajustes aparece en la sección **Propiedades**.
4. Utilice campos **patrón de inicio** y **patrón parada** para especificar los datos que define el inicio y el final de un recibo.
5. Haga clic en **Iniciar a recopilar datos** para recopilar datos sin procesar de la fuente de datos conectada. Cuanto más datos que recopila, menor será el riesgo de caracteres que faltan, por ejemplo, los caracteres de control, que desea reemplazar u omitir.

6. En la sección de **datos sin procesar**, resalte los caracteres que desea reemplazar u omitir. Si desea escribir los caracteres manualmente, omita este paso y haga clic en **Añadir filtro**.
7. Haga clic en **Añadir filtro** para definir cómo se muestran los caracteres seleccionados de los datos de origen de la transacción en XProtect Smart Client.
8. Para cada filtro, seleccione una acción para determinar cómo se transforman los personajes. La sección **previsualización** le da una vista previa de cómo los datos son presentados con los filtros definidos.

Para obtener información detallada sobre los campos, consulte Definiciones de transacción (propiedades) (en la página 380).

También puede cargar los datos recogidos previamente almacenados localmente en el equipo. Para ello, haga clic **la carga del archivo**.

Definiciones de transacción (propiedades)

Los ajustes para las definiciones de las transacciones se describen en la tabla.

Nombre	Descripción
Nombre	Escriba un nombre.
Codificación	Seleccione el conjunto de caracteres utilizado por el origen de la transacción, por ejemplo, la caja registradora. Esto ayuda a que XProtect Transact convierta los datos de transacción en texto comprensible con el que pueda trabajar al configurar la definición. Si selecciona la codificación incorrecta, los datos pueden aparecer como texto sin sentido.
Iniciar la recogida de datos	Recoger datos de la transacción desde el origen de la transacción conectada. Puede utilizar los datos para configurar una definición de transacción. Espere por lo menos uno, pero preferiblemente más, para completar las transacciones.
Detener la recopilación de datos	Cuando se han recogido datos suficientes para configurar la definición, haga clic en este botón.
La carga del archivo	Si desea importar datos de un archivo existente, haga clic en este botón. Normalmente se trata de un archivo que ha creado previamente en el formato de archivo . capture. Puede haber otros formatos de archivo. Lo que es importante aquí es que la codificación del archivo de importación coincide con la codificación seleccionada para la definición actual.
Guardar en el archivo	Si desea guardar los datos brutos recogidos en un archivo, haga clic en este botón. Puede volver a utilizar más adelante.

Nombre	Descripción
Tipo de partida	Seleccione el tipo de concordancia de usar para buscar la máscara de inicio y parada de la máscara en los datos brutos recogidos: • Utilizar la concordancia exacta: La búsqueda identifica cadenas que contengan exactamente lo que ha entrado en campos **máscara inicio** y la **máscara de parada**. • Utilizar comodines: La búsqueda identifica cadenas que contienen lo que ha introducido en los campos **Máscara inicial** y **Máscara de detención** en combinación con un símbolo de comodín (*, #, ?). * Coincide cualquier número de caracteres. Por ejemplo, si ha entrado en "Iniciar * ción d", la búsqueda identifica cadenas que contienen "Iniciar la transacción". # Coincide exactamente 1 dígito. Por ejemplo, si ha introducido "# sandía", la búsqueda identifica cadenas que contienen, por ejemplo, "1 sandía". ? coincide exactamente con 1 personaje. Por ejemplo, puede usar la expresión de búsqueda "Inicio trans?cción" para identificar cadenas que contienen "Iniciar transacción". • Utilizar expresiones regulares: Utilizar este tipo de concordancia para identificar cadenas que contienen los métodos de notación o convenciones específicas, por ejemplo, un formato de fecha o número de tarjeta de crédito. Para obtener más información, consulte el sitio web de Microsoft (https://msdn.microsoft.com/en-us/library/az24scfc(v=vs.110).aspx).
Los datos en bruto	Cadenas de datos de transacciones desde el origen de la transacción conectados se muestran en esta sección.
Iniciar la máscara	Especificar una máscara de inicio para indicar dónde comienza una transacción. Las líneas horizontales se insertan en el campo **Previsualizar** para visualizar donde la transacción comienza y termina, y ayudará a mantener las transacciones individuales separados.
Máscara de parada	Especificar una máscara de parada para indicar dónde termina una transacción. Una máscara de parada no es obligatoria, pero es útil si los datos recibidos contienen información irrelevante, tal como información sobre los horarios de apertura u ofertas especiales, entre las transacciones reales. Si no se especifica una máscara de parada, al final de la recepción se define en términos de dónde comienza el siguiente recibo. El inicio está determinado por lo que se ingresa en campo **inicio enmascarar**.
Añadir filtro	Usa los filtros **Añadir** botón para señalar los caracteres que desea que se omite en XProtect Smart Client o sustituidos por otros caracteres o un salto de línea. Sustitución de caracteres es útil cuando la cadena de origen de transacciones contiene caracteres de control con fines de no impresión. Adición de saltos de líneas es necesario hacer recibos de XProtect Smart Client se asemejan a los recibos originales.

Nombre	Descripción
Texto de filtro	Muestra los caracteres actualmente seleccionados en la sección de **datos sin procesar**. Si conoce caracteres que desea omitir o reemplazar, pero no ocurren en la cadena de datos sin procesar, puede introducir los caracteres manualmente en el campo **Caracter**. Si el carácter es un carácter de control, es necesario introducir su valor de byte hexadecimal. Utilice este formato para el valor de byte: {XX} y {XX, XX, . . . } si un carácter se compone de más bytes.
Acción	Para cada filtro se agrega, debe especificar cómo se manejan los caracteres que ha seleccionado: • Omiten: los caracteres que seleccione se filtran. • Sustitutos: los caracteres que seleccione se sustituyen por los caracteres que especifique. • Añadir salto de línea: los caracteres seleccionados se sustituyen por un salto de línea.
Sustitución	Escriba el texto para reemplazar los caracteres seleccionados. Sólo es relevante si se ha seleccionado la acción **Sustituto**.
Previsualizar	Utilice la sección **Prever** para verificar que ha identificado y filtrado los caracteres no deseados. La salida que se ve aquí se asemeja a lo que el recibo de la vida real se ve como en XProtect Smart Client.

Ver también

Añadir transacción definiciones (en la página 379)

Configuración de eventos de transacciones y alarmas

En esta sección, aprenderá cómo definir los eventos de transacciones y configurar alarmas.

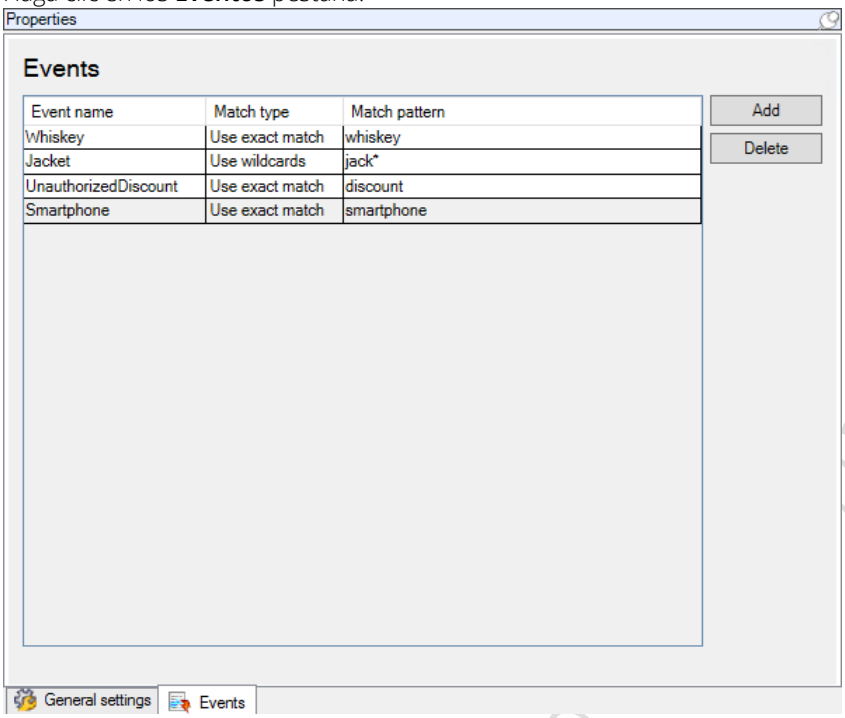
Definir eventos de transacción

Para realizar el seguimiento e investigar los eventos de transacción en XProtect Smart Client, primero es necesario definir lo que los eventos son, por ejemplo, la adquisición de un teléfono inteligente. Se define eventos de transacciones en una definición de transacción, de modo que los eventos definidos se aplican a todas las fuentes de transacción, por ejemplo, cajas registradoras, que utilizan la definición transacción.

Pasos:

1. En el **Panel Navegación del sitio**, expanda **Transact**.

2. Ir al panel general. Seleccione la definición de la transacción, donde desea definir un evento.
3. Haga clic en los **Eventos** pestaña.



4. En el panel **Propiedades**, haga clic en **Añadir**. Se añade una nueva línea.
5. Escriba un nombre para el evento.
6. Seleccione el tipo de concordancia de utilizar para identificar una cadena específica en los datos de la transacción como un evento. Se puede elegir entre coincidencia exacta, símbolos comodines y expresiones regulares. Para obtener más información, consulte la descripción del tipo de concordancia en Definiciones de transacción (propiedades) (en la página 380).
7. En la columna **Patrón de coincidencia**, especifique qué desea que el sistema identifique como un evento, por ejemplo, "smartphone".
8. Para cada caso, repita los pasos anteriores.

Ver también

Reglas y eventos (explicado) (en la página 184)

Definiciones de transacciones (explicadas) (en la página 375)

Cree alarmas basadas en eventos de transacciones

Para notificar al operador XProtect Smart Client cuando se produce un suceso de transacción específico, primero debe crear una alarma de transacción en Management Client. La alarma aparecerá en pestaña **Administrador de alarmas** de XProtect Smart Client permite al operador para investigar el caso y, si es necesario, tomar medidas.

Pasos:

1. En el **Panel Navegación del sitio**, expanda **Alarmas**.

2. Ir al panel general. Haga clic con el botón derecho del ratón en el nodo **Definiciones de alarma** y seleccione **Añadir nuevo...**. Los ajustes en las **propiedades** panel se activan.
3. Escriba un nombre para la alarma y, en el campo **Descripción**, posiblemente también instrucciones para el operador de XProtect Smart Client sobre qué acción tomar.
4. En menú desplegable **evento desencadenante**, seleccione **Eventos de transacción**.
5. En el menú desplegable a continuación **Eventos de transacción**, seleccione el evento específico.
6. En el campo **Fuentes**, haga clic en el botón **Seleccionar...**. Aparece una ventana emergente.
7. Haga clic en pestaña **Servidores** y seleccione el origen de la transacción.
8. Especificar opciones adicionales. Para obtener más información, consulte Definiciones de alarma (ver "Definiciones de alarma (propiedades)" en la página 277).

Ver también

Definir eventos de transacción (en la página 382)

Configurar reglas en un evento

Para activar una acción cuando se produce un evento de transacción específica, es necesario configurar una regla, donde se selecciona un evento y especifica lo que debe suceder, por ejemplo, que una cámara empieza a grabar o un e-mail se envía.

Pasos:

1. En el **Panel Navegación del sitio**, expanda **Reglas y eventos**.
2. Ir al panel general. Haga clic con el botón derecho del ratón en **Reglas** y seleccione **Añadir Regla...**. Aparece un asistente.
3. Siga los pasos del asistente.
4. Asegúrese de que el **realizar una acción sobre se selecciona <evento>** botón de radio.
5. Seleccione el evento de transacción de conformidad **Transact** > **eventos de transacción**.
6. Si una acción tiene lugar la grabación, y desea utilizar las cámaras asociadas a las fuentes de transacción, por ejemplo, las cajas registradoras, seleccione los dispositivos **uso de metadatos** botón de opción en el cuadro de diálogo que aparece durante el asistente.

Ver también

Definir eventos de transacción (en la página 382)

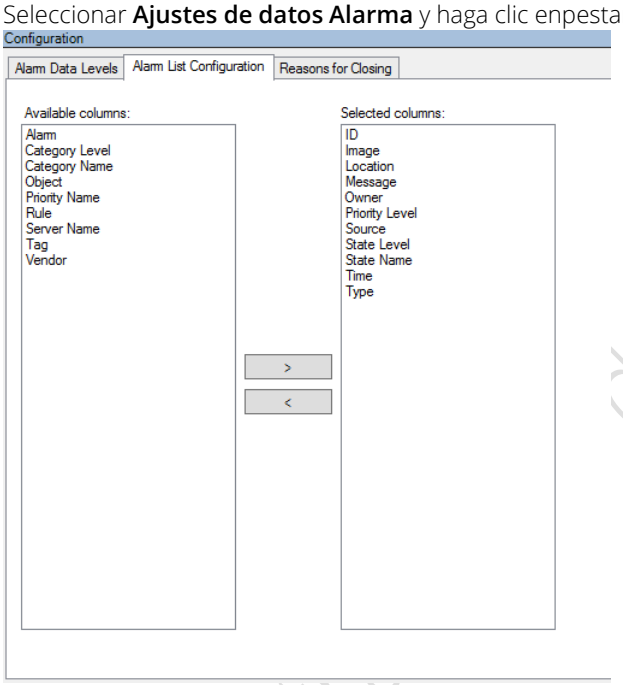
Reglas y eventos (explicado) (en la página 184)

Habilitar el filtrado de eventos de transacciones o alarmas

Si desea que el operador XProtect Smart Client pueda filtrar eventos o alarmas por transacciones, primero debe habilitar el campo **Tipo** en Management Client. Una vez activado, el campo está disponible en la sección de filtro en la pestaña **Administrador de alarmas** de XProtect Smart Client.

Pasos:

1. En el **Panel Navegación del sitio**, expanda **Alarmas**
2. Seleccionar **Ajustes de datos Alarma** y haga clic enpestaña **lista de configuración alarma**.



3. En sección **columnas disponibles**, seleccione el campo **Tipo**.
4. Añadir el campo para **columnas seleccionadas**.
5. Guardar los cambios. Ahora, el campo está disponible en XProtect Smart Client.

El mantenimiento de la configuración de transacciones

En esta sección, aprenderá cómo editar, desactivar y eliminar las fuentes de transacción.

Editar configuración de la fuente de transacción

Después de la adición de una fuente de transacción, puede cambiar el nombre o seleccione una definición de transacción diferente. En función del conector seleccionado, puede haber ajustes adicionales que se pueden modificar, por ejemplo, el nombre de host y el número de puerto de un servidor TCP conectado. Además, se puede desactivar una fuente de transacción. Esto interrumpe el flujo de datos de la transacción desde el origen de la transacción al servidor de eventos.

Una vez que haya seleccionado un conector, no se puede cambiar.

Pasos:

1. En el **Panel Navegación del sitio**, expanda **Transact**.
2. Seleccionar **fuentes de transacción**.
3. Ir al panel general. Haga clic en el origen de la transacción. Las propiedades se muestran.
4. Realice los cambios necesarios y guardarlos. Para obtener más información, consulte fuentes de transacción (propiedades) (en la página 378).

Ver también

Añadir origen de la transacción (asistente) (en la página 377)

Deshabilitar fuentes de transacción (en la página 386)

Deshabilitar fuentes de transacción

Puede desactivar una fuente de transacciones, por ejemplo, si un cajero automático está temporalmente fuera de servicio, o un servicio en una caja registradora registrada está deshabilitado. El flujo de datos de la transacción al servidor de eventos se interrumpe.

Pasos:

1. En el **Panel Navegación del sitio**, expanda **Transact**.
2. Seleccionar **fuentes de transacción**.
3. Ir al panel general. Haga clic en el origen de la transacción. Las propiedades se muestran.
4. Desactive la casilla de verificación **Habilitar** y guarde los cambios. El origen de la transacción está deshabilitado.

Ver también

Añadir origen de la transacción (asistente) (en la página 377)

Eliminar origen de la transacción (ver "Eliminar fuentes de transacción" en la página 386)

Eliminar fuentes de transacción

Puede eliminar las fuentes de transacción que haya añadido. Los datos de transacción almacenados de esa fuente se eliminan del servidor de eventos.

Como alternativa, puede desactivar la fuente de transacciones para evitar que se eliminan los datos de transacción almacenados. Una fuente de transacciones con discapacidad también requiere una licencia de código de transacción.

Pasos:

1. En el **Panel Navegación del sitio**, expanda **Transact**.
2. Seleccionar **fuentes de transacción**.
3. Ir al panel general. Haga clic en el artículo **Fuentes de transacción**. Haga clic en la fuente que desea eliminar.
4. Seleccione **Borrar**. Aparece un cuadro de diálogo.

5. Haga clic en **OK** para confirmar que desea eliminar la fuente de transacción.

Ver también

Añadir origen de la transacción (asistente) (en la página 377)

Verificar la configuración de XProtect Transact

Cuando haya terminado de configurar XProtect Transact y sus componentes, puede probar que Transact funciona como se esperaba en XProtect Smart Client.

1. Compruebe que todas las fuentes de transacción necesarias se han agregado correctamente en Management Client:
    1. Abra XProtect Smart Client y haga clic en la ficha **Transact**.
    2. Haga clic en el **Todas las fuentes** menú desplegable y verificar que todas las fuentes de transacción aparecen.
2. Compruebe que las definiciones de transacción se han configurado correctamente en Management Client. Si se ha configurado correctamente, hay un recibo por la transacción, y las líneas de rotura correctamente:
    1. Abra XProtect Smart Client y haga clic en la ficha **Transact**.
    2. Seleccione una fuente de transacción que sepa que está activa y haga clic en  . Las líneas de transacción para hoy aparecen.
    3. Haga clic en una línea para ver las grabaciones de recepción y de vídeo asociados.
3. Verificar que la transacción eventos están configurados correctamente:
    1. Defina un evento de prueba de transacción en Management Client, por ejemplo un elemento que es probable que se compre y se registre en una fuente de transacción conectada, por ejemplo una caja registradora.
    2. Cuando se ha producido el evento, abra XProtect Smart Client y haga clic en pestaña **Administrador de alarma**.
    3. Abra la lista de alarmas y seleccione **Evento**. Los eventos más recientes se muestran en la parte superior de la lista. El evento de prueba que ha creado debería aparecer en la lista.

Milestone Mobile

Introducción Milestone Mobile

Milestone Mobile (explicado)

Milestone Mobile consta de tres componentes:

- **Cliente Milestone Mobile**
- **Servidor Milestone Mobile**
- **Plug-in Milestone Mobile**

El cliente Milestone Mobile es una aplicación de vigilancia móvil que puede instalar y utilizar en su dispositivo Android, dispositivo Apple o dispositivo Windows Phone. Puede utilizar tantas instalaciones de cliente Milestone Mobile como sea necesario.

Para obtener más información, descargue la Guía del usuario del cliente de Milestone Mobile desde el sitio web (http://www.milestonesys.com/support/manuals-and-guides/) de Milestone Systems.

El servidor Milestone Mobile y Milestone Mobile plug-in están cubiertos en este manual.

Requisitos para utilizar Milestone Mobile

Antes de poder empezar a utilizar Milestone Mobile, usted debe asegurarse de que tiene lo siguiente:

- Un VMS corriendo instalado y configurado con al menos un usuario.
- Cámaras y vistas configuradas en XProtect Smart Client.
- Un dispositivo móvil con Android, iOS o Windows con acceso a Google Play, App Store℠ o Windows Phone Store desde donde se puede descargar la aplicación cliente de Milestone Mobile.

Requisitos del sistema Milestone Mobile

Para obtener información acerca de los **requisitos mínimos del sistema** a los diversos componentes, vaya al sitio web (https://www.milestonesys.com/support/resources/system-requirements) Milestone.

- Para encontrar los requisitos para el cliente Milestone Mobile, haga clic en la entrada **Milestone Mobile**.
- Para encontrar los requisitos para el servidor Milestone Mobile, haga clic en el producto XProtect que ha instalado.
- Los requisitos para el complemento Milestone Mobile son:
  - Un Management Client en ejecución.
  - El complemento Milestone está instalado para integrarse con su VMS.

Configuración Milestone Mobile

Servidor Milestone Mobile (explicado)

El servidor Milestone Mobile gestiona los inicios de sesión del sistema desde Milestone Mobile desde un dispositivo móvil o XProtect Web Client.

Un servidor Milestone Mobile distribuye secuencias de vídeo de servidores de grabación al clientes Milestone Mobile. Esto ofrece una configuración segura donde los servidores de grabación nunca se conectan a Internet. Cuando un servidor Milestone Mobile recibe secuencias de vídeo de la grabación de los servidores, sino que también se encarga de la conversión del complejo de codecs y formatos que permiten el streaming de vídeo en el dispositivo móvil.

Debe instalar el servidor Milestone Mobile en cualquier ordenador desde el que desea acceder a servidores de grabación. Al instalar el servidor Milestone Mobile, asegúrese de que inicie sesión con una cuenta que tenga derechos de administrador. De lo contrario, la instalación no se realiza correctamente.

Milestone Federated Architecture y servidores maestro / esclavo (explicado)

Si el sistema es compatible Milestone Federated Architecture o servidores en una configuración maestro/esclavo, puede acceder a dichos servidores con su cliente Milestone Mobile. Utilizar esta funcionalidad para acceder a todas las cámaras de todos los servidores esclavos iniciando sesión en el servidor maestro.

Si en una configuración de Milestone Federated Architecture, se accede a los sitios secundarios a través del sitio central. Instalar el servidor Milestone Mobile sólo en el sitio central.

Esto significa que cuando los usuarios del cliente Milestone Mobile iniciar sesión en un servidor para ver las cámaras de todos los servidores en el sistema, deben conectarse a la dirección IP del servidor maestro. Los usuarios deben tener derechos de administrador en todos los servidores del sistema a fin de que las cámaras que se muestran en el cliente Milestone Mobile.

Conexión inteligente (explicada)

Smart Connect le permite verificar que ha configurado el servidor Mobile correctamente sin iniciar sesión con un dispositivo móvil o una tableta para realizar la validación. También simplifica el proceso de conexión para los usuarios del cliente.

Esta función requiere que su servidor Milestone Mobile utilice una dirección IP pública y que su sistema tenga licencia con un paquete de suscripción Milestone Care Plus.

El sistema le da una respuesta instantánea en el Management Client si la configuración de conectividad remota se ha configurado satisfactoriamente y confirma que el Mobile Server es accesible desde Internet.

Smart Connect permite al servidor Milestone Mobile cambiar sin problemas entre direcciones IP internas y externas y conectarse al servidor Mobile desde cualquier ubicación.

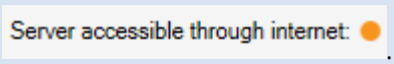
Para facilitar la configuración de los clientes Mobile de los clientes, puede enviar un correo electrónico directamente desde el Management Client al usuario final. El correo electrónico incluye un enlace que agrega el servidor directamente a Milestone Mobile. Esto completa la configuración sin necesidad de introducir direcciones de red o puertos.

Puesta en funcionamiento de Smart Connect

Habilitar Universal Plug and Play de descubrimiento en el router

Para que sea más fácil de conectar dispositivos móviles a servidores Milestone Mobile, puede habilitar Universal Plug and Play (UPnP) en el router. UPnP permite servidor Milestone Mobile para configurar el reenvío de puertos

de forma automática. Sin embargo, también se puede configurar manualmente el reenvío de puertos en el router mediante el uso de su interfaz web. Dependiendo del router, el proceso para establecer un mapa de puertos puede ser diferente. Si no está seguro de cómo configurar el reenvío de puertos en el router, consulte la documentación de dicho dispositivo.

Nota: Cada cinco minutos, el servicio de servidor Milestone Mobile verifica que el servidor está disponible para los usuarios en Internet. El estado se muestra en la esquina superior izquierda de la **Propiedades** panel: 

.

Requisitos

- Su servidor Milestone Mobile debe utilizar una dirección IP pública. La dirección IP puede ser estática o dinámica, pero normalmente lo mejor es usar direcciones IP estáticas.
- Debe tener una licencia válida para Smart Connect.

Configurar los ajustes de conexión

1. En Management Client, en el panel de navegación, expanda **Servidores** y seleccione **Mobile Server**.
2. Seleccione el servidor y haga clic en la pestaña **Conectividad**.
3. Utilice las opciones en el grupo **general** para especificar lo siguiente:
   - Para que sea más fácil para los usuarios conectar dispositivos móviles a los servidores Milestone Mobile, seleccione la casilla de verificación **Smart Connect Habilitar** .
   - Especificar el protocolo a utilizar en el campo **Tipo de conexión**.
   - **Nota:** Si activa las conexiones seguras, dispositivos Windows Phone, pueden conectarse sólo si tiene un certificado de una autoridad de certificación (CA) instalado en el servidor de Milestone Mobile. Cuestión entidades emisoras de certificados digitales que verifican las identidades de los usuarios y los sitios web que intercambian datos a través de Internet. Ejemplos de entidades emisoras son empresas como Comodo, Symantec, y GoDaddy.
   - Antes de encender conexiones seguras, asegúrese de que está familiarizado con los certificados digitales. Para aprender a añadir un certificado de servidor de Milestone Mobile, ver editar certificados (ver "Editar certificado" en la página 409).
   - Especifique el número de segundos antes de que los tiempos de espera de la conexión.
   - Para permitir que los dispositivos móviles se encuentran los servidores Milestone Mobile que se encuentran dentro del alcance, seleccione el cuadro de verificación **Habilitar UPnP detectabilidad**.
   - Para permitir que los enrutadores para reenviar los dispositivos móviles a un puerto específico, seleccione el cuadro de verificación **Habilitar asignación de puertos automática**.

Enviar un mensaje de correo electrónico para ayudar a los usuarios se conectan

Puede que sea fácil para los usuarios para empezar con Milestone Mobile mediante el envío de un mensaje de correo electrónico que incluye información de conexión. Puede enviar el mensaje directamente desde Management Client, o puede copiar la información al programa de mensajería que utiliza.

1. En el campo **Invitación por correo electrónico a**, introduzca la dirección de correo electrónico del destinatario, y luego especificar un idioma.

2. A continuación, lleve a cabo uno de los siguientes:
   - Para enviar el mensaje, haga clic en **Enviar**.
   - Copiar la información en el programa de mensajería que utiliza.

Habilitar conexiones en una red compleja

Si tiene una red compleja donde tiene ajustes personalizados, puede proporcionar la información que los usuarios necesitan para conectarse.

En el grupo **Acceso a Internet**, especifique lo siguiente:

- Si utiliza la asignación de puertos UPnP, a conexiones directas a una conexión específica, seleccione la casilla de verificación **configurar el acceso a Internet a medida**. A continuación, proporcione la **dirección IP o nombre de host** y el puerto que se utilizará para la conexión. Por ejemplo, puede hacerlo si su router no es compatible con UPnP, o si tiene una cadena de routers.
- Si las direcciones IP cambian a menudo, seleccione la casilla de verificación **Comprobar dinámicamente para recuperar la dirección IP**.

Envío de notificaciones (explicado)

Puede activar Milestone Mobile para notificar a los usuarios cuando se produce un evento, por ejemplo, cuando una alarma se dispara o algo va mal con un dispositivo o servidor. Las notificaciones siempre se entregan, independientemente de si la aplicación se está ejecutando o no. Cuando Milestone Mobile está abierto en el dispositivo móvil, la aplicación ofrece la notificación. Las notificaciones del sistema también se entregan incluso cuando la aplicación no se está ejecutando. Los usuarios pueden especificar los tipos de notificaciones que desean recibir. Por ejemplo, un usuario puede elegir recibir las notificaciones de los siguientes:

- Todas las alarmas
- Sólo se asignan alarmas
- Sólo las alarmas relacionadas con el sistema. Estos podrían ser cuando un servidor se desconecta o vuelve a estar conectado.

También puede utilizar las notificaciones push para notificar a los usuarios que no tienen abierta Milestone Mobile. Éstos se llaman las notificaciones push. Notificaciones push se entregan al dispositivo móvil, y son una gran manera de mantener informados a los usuarios mientras están en movimiento.

El uso de las notificaciones push

Nota: Para utilizar las notificaciones push, el sistema debe tener acceso a Internet.

Notificaciones push utilizan servicios en la nube de Apple, Microsoft y Google:

- Servicio Apple Push Notification (APN)
- Centro de notificación de Microsoft Azure
- Servicio Google Cloud Messaging Push Notification

Hay un límite en el número de notificaciones que se permite su sistema para enviar durante un período de tiempo. Si el sistema supera el límite, se puede enviar sólo una notificación cada 15 minutos durante el próximo período. La notificación contiene un resumen de los eventos que ocurrieron durante los 15 minutos. Después de que el período siguiente, se elimina la limitación.

Configurar el envío de notificaciones a dispositivos móviles

Puede activar Milestone Mobile para notificar a los usuarios cuando se produce un evento, por ejemplo, cuando una alarma se dispara o algo va mal con un dispositivo o servidor.

Requisitos

- Debe asociar una o más alarmas con uno o más eventos y reglas. Esto no es necesario para las notificaciones del sistema.
- Asegúrese de que su contrato de Milestone Care™ con Milestone Systems es de hasta al día.
- Su sistema debe tener acceso a Internet.

Configurar las notificaciones del sistema

Para enviar notificaciones relacionadas con el sistema, como cuando un servidor se desconecta, siga estos pasos:

1. En Management Client, seleccione el servidor Mobile y, a continuación, haga clic en la pestaña **Notificaciones**.
2. Seleccione la casilla de verificación **Notificaciones**.

Configurar las notificaciones en el servidor Milestone Mobile

Para configurar las notificaciones, siga estos pasos:

1. En Management Client, seleccione el servidor Mobile y, a continuación, haga clic en la pestaña **Notificaciones**.
2. Para enviar notificaciones a todos los dispositivos móviles que se conectan al servidor, seleccione la casilla de verificación **Notificaciones**.
3. Para almacenar información acerca de los usuarios y dispositivos móviles que se conectan al servidor, active la casilla de verificación **Actualizar dispositivo**.

Nota: El servidor envía notificaciones sólo a los dispositivos móviles en esta lista. Si desactiva la casilla de verificación **Actualizar dispositivo** y guardar el cambio, el sistema borra la lista. Para recibir notificaciones de inserción de nuevo, los usuarios deben conectar sus dispositivos.

Detener el envío de notificaciones de inserción a dispositivos móviles específicos o todos los dispositivos móviles

Hay varias formas de detener el envío de notificaciones de inserción a dispositivos móviles.

1. En Management Client, seleccione el servidor Mobile y, a continuación, haga clic en la pestaña **Notificaciones**.
2. Puede seguir estos pasos:
   - Para dispositivos individuales, desactive la casilla de verificación **Activado** para cada dispositivo móvil. El usuario puede utilizar otro dispositivo para conectar con el servidor Milestone Mobile.
   - Para todos los dispositivos, desactive la casilla de verificación **Notificaciones**.

Para detener temporalmente todos los dispositivos, desactive la casilla de verificación **Actualizar dispositivo** y guardar el cambio. El sistema envía notificaciones a los usuarios de nuevo después de volver a conectar.

Establecer investigaciones

Establezca investigaciones para que las personas puedan usar Web Client y Milestone Mobile para acceder a videos grabados e investigar incidentes, y preparar y descargar evidencia de vídeo.

Para configurar las investigaciones, siga estos pasos:

1. En Management Client, haga clic en el servidor Mobile y, a continuación, haga clic en la pestaña **Investigaciones**.
2. Active la casilla de verificación **Habilitada**. De forma predeterminada, se selecciona la casilla de verificación.
3. En el campo **Investigaciones carpeta**, especifique dónde almacenar el video para las investigaciones.
4. En el campo **Limitar el tamaño de las investigaciones al campo** , escriba el número máximo de megabytes que puede contener la carpeta de investigación.
5. Opcional: Para permitir a los usuarios acceder a las investigaciones que otros usuarios crean, seleccione la casilla de verificación **Ver investigaciones realizadas por otros usuarios**. Si no selecciona esta casilla, los usuarios sólo pueden ver sus propias investigaciones.
6. Opcional: Para incluir la fecha y hora en que un vídeo se ha descargado, seleccione el **Incluir marcas de tiempo para AVI exporta** casilla de verificación.
7. En el **códec utilizado para AVI exporta** campo, seleccione el formato de compresión para usar en la preparación de paquetes de AVI para su descarga.

   Nota: Los códecs de la lista pueden ser diferentes, dependiendo de su sistema operativo. Si no ve el códec que desea utilizar, puede instalarlo en el equipo donde Management Client se está ejecutando y se mostrará en esta lista.

   Además, los codecs pueden utilizar diferentes tasas de compresión, que pueden afectar la calidad de vídeo. Tasas de compresión más altas reducen los requisitos de almacenamiento, pero también puede reducir la calidad. Tasas de compresión más bajas requieren más capacidad de almacenamiento y de red, pero pueden aumentar la calidad. Es una buena idea investigar los códecs antes de seleccionar uno.
8. En el campo **Guardar o eliminar datos cuando las exportaciones fallan (MKV y AVI)** campo, especifique si desea conservar los datos que se descargaron correctamente, aunque pueden ser incompletos o eliminarlos.
9. Para permitir a los usuarios guardar las investigaciones, debe conceder el permiso **Exportar** al rol de seguridad asignado a los usuarios.

Limpiar las investigaciones

Si usted tiene investigaciones o las exportaciones de vídeo que ya no necesita para mantener, puede eliminarlos. Por ejemplo, esto puede ser útil si desea hacer más espacio en disco disponible en el servidor.

- Para eliminar una investigación, y todas las exportaciones de vídeo que se han creado para ello, seleccione la investigación en la lista y, a continuación, haga clic en **Eliminar**.

- Para eliminar archivos de vídeo individuales que se exportaron a cabo una investigación, pero manteniendo la investigación, seleccione la investigación en la lista. En el grupo **detalles de la investigación**, haga clic en el icono **Eliminar** a la derecha de la **base de datos**, **AVI**, **MKV** o campos para la exportación.

Utilización de Video Push para transmitir vídeo (explicado)

Puede configurar vídeo empuje para que los usuarios puedan mantener informados a los demás acerca de una situación, o grabar un vídeo para investigar más tarde, por la transmisión de vídeo desde la cámara de su dispositivo móvil al sistema de vigilancia XProtect.

Configurar empuje video para transmitir vídeo

Para permitir que los usuarios transmitan vídeo desde sus dispositivos móviles al sistema XProtect, configure Video Push en el servidor Milestone Mobile.

Requisitos

- Cada canal requiere una licencia de dispositivo de hardware.

En Management Client, realice estos pasos en el orden siguiente:

1. Establecer un canal que el dispositivo móvil puede usar para transmitir vídeo al servidor de grabación.
2. Añadir el controlador de vídeo de empuje como un dispositivo de hardware en el servidor de grabación. El controlador simula un dispositivo de cámara para que pueda transmitir vídeo al servidor de grabación.
3. Asignar el dispositivo controlador de vídeo Pulsar para el canal.

En este tema se describe cada uno de estos pasos.

Establecer un canal de video streaming

Para añadir un canal, siga estos pasos:

1. En el panel de navegación, seleccione **Mobile Server** y seleccione el servidor Mobile.
2. En la ficha **Vídeo** empuje, seleccione la casilla de verificación **vídeo empuje**.
3. En la esquina inferior derecha, haga clic en **Añadir** para añadir un canal de vídeo bajo presión **mapeo canales**.
4. Introduzca el nombre de usuario de la cuenta de usuario (agregado bajo **Cometidos**) que utilizará el canal. Esta cuenta de usuario debe tener permiso para acceder al servidor Milestone Mobile y al servidor de grabación (en la pestaña **Seguridad general**).

   Nota: Para utilizar empuje del vídeo, los usuarios deben iniciar sesión en Milestone Mobile en su dispositivo móvil utilizando el nombre de usuario y la contraseña para esta cuenta.

5. Anote el número de puerto. Lo necesitará cuando se agrega el controlador de vídeo de empuje como un dispositivo de hardware en el servidor de grabación.
6. Haga clic en **OK** para cerrar el cuadro de diálogo de video del canal de empuje y el guardar el canal.

Añadir el controlador de vídeo de empuje como un dispositivo de hardware en el servidor de grabación.

1. En el panel de navegación, haga clic en **servidores de grabación**.
2. Haga clic en el servidor que desea transmitir vídeo ay, haga clic en **Añadir hardware** para abrir el asistente **Añadir hardware**.
3. Seleccionar **manual** como el método de detección de hardware y haga clic en **Siguiente**.
4. Introduzca las credenciales para la cámara, de la siguiente manera:
   - Para el nombre de usuario, ingrese los valores predeterminados de fábrica o el nombre de usuario especificado en la cámara.
   - Por contraseña: Escriba Milestone y, a continuación, haga clic en **Siguiente**.

   Nota: Estas son las credenciales para el hardware, no para el usuario. Ellos no están relacionados con el nombre de usuario para el canal.
5. En la lista de controladores, ampliar **Otros**, seleccione la casilla de verificación **vídeo empuje controlador**, y luego haga clic en **Siguiente**.

   Nota: El sistema genera una dirección MAC para el dispositivo de vídeo empuje del controlador. Recomendamos que utilice esta dirección. Cambiar sólo si experimenta problemas con el dispositivo de vídeo empuje del controlador. Por ejemplo, si necesita añadir una nueva dirección y número de puerto.
6. En el campo **Dirección**, ingrese la dirección IP del equipo donde está instalado el servidor Milestone Mobile.
7. En el campo **Puerto**, ingrese el número de puerto para el canal que creó para el streaming de vídeo. El número de puerto se le asignó cuando se creó el canal.
8. En la columna de la **Modele de hardware**, seleccione **vídeo empuje controlador** y, a continuación, haga clic en **Siguiente**.
9. Cuando el sistema detecta el nuevo hardware, haga clic en **Siguiente**.
10. En el campo **Patrón del nombre de hardware** especifique si desea mostrar ya sea el modelo del hardware y la dirección IP, o sólo el modelo.
11. Especifique si desea activar los dispositivos relacionados seleccionando la casilla de verificación **Habilitada**. Puede añadir dispositivos relacionados a la lista para **Video Push Driver**, aunque no estén habilitados. Puede activar más tarde.

    Nota: Si desea utilizar la información de ubicación cuando secuencia de vídeo, debe habilitar el puerto **metadatos**.
12. Seleccione los grupos predeterminados para los dispositivos relacionados a la izquierda o seleccione un grupo específico en el campo **Añadir al grupo**. Adición de dispositivos a un grupo puede hacer que sea más fácil de aplicar los ajustes a todos los dispositivos al mismo tiempo o el uso de instalaciones.

Añadir el dispositivo controlador de vídeo Pulsar para el canal de empuje de vídeo

1. En el panel **navegación del sitio**, haga clic en **Servidores Mobile** y, a continuación, haga clic en la pestaña **Empuje vídeo**.

2. Haga clic en **Buscar cámaras**. Si tiene éxito, el nombre de la cámara de vídeo del controlador de empuje aparece en el campo **Nombre de la cámara**.

3. Guardar la configuración.

Retirar un canal que no es necesario

Puede eliminar canales que ya no utilice.

- Seleccione el canal de quitar y, a continuación, haga clic en **Quitar** en la esquina inferior derecha.

Configurar usuarios para la Doble verificación de acceso por correo electrónico

Funcionalidad disponible depende del sistema que está utilizando. Ver tabla de comparación de productos (en la página 24) para más información.

Para imponer un paso de inicio de sesión adicional a los usuarios del cliente Milestone Mobile o XProtect Web Client, configure la Doble verificación de acceso en el servidor Milestone Mobile. Además del nombre de usuario y contraseña estándar, el usuario debe ingresar un código de verificación recibido por correo electrónico.

Doble verificación de acceso aumenta el nivel de protección de su sistema de vigilancia.

Requisitos

- Ha instalado un servidor SMTP.
- Ha añadido usuarios y grupos a su sistema XProtect en el Management Client en el nodo **Cometidos** en el panel **Navegación del sitio**. En el rol relevante, seleccione la pestaña **Usuarios y grupos**.
- Si actualizó su sistema de una versión anterior de XProtect, debe reiniciar el servidor Mobile para habilitar la función de Doble verificación de acceso.

En Management Client, realice estos pasos:

1. Ingrese información sobre su servidor SMTP.
2. Especifique la configuración del código de verificación que se enviará a los usuarios del cliente.
3. Asigne el método de inicio de sesión a usuarios y grupos de dominio.

En este tema se describe cada uno de estos pasos.

Ingrese información sobre su servidor SMTP

El proveedor utiliza la información sobre el servidor SMTP:

1. En el panel de navegación, seleccione **Servidores Mobile** y seleccione el servidor Mobile correspondiente.
2. En la ficha **Doble verificación de acceso**, seleccione la casilla de verificación **Activar Doble verificación de acceso**.
3. Debajo de **Configuración del proveedor**, en la ficha **Correo electrónico**, introduzca información acerca de su servidor SMTP y especifique el correo electrónico que enviará el sistema a los usuarios del cliente cuando inicien sesión y se configuren para un inicio de sesión secundario. Para obtener más información sobre cada parámetro, consulte Doble verificación de acceso (en la página 406).

Especifique el código de verificación que se enviará a los usuarios

Para especificar la complejidad del código de verificación:

1. En la ficha **Doble verificación de acceso**, en la **configuración de códigos de verificación** sección, especifique el período dentro del cual los usuarios de Milestone Mobile, no tiene que volver a verificar su inicio de sesión en caso de, por ejemplo, una red desconectada. El período predeterminado es de 3 minutos.
2. Especifique el período dentro del cual el usuario puede utilizar el código de verificación recibido. Después de este período, el código no es válido y el usuario tiene que solicitar un nuevo código. El período predeterminado es de 5 minutos.
3. Especifique el número máximo de intentos de entrada de código antes de bloquear el usuario. El número predeterminado es 3.
4. Especifique el número de caracteres para el código. La longitud predeterminada es 6.
5. Especifique la complejidad del código que desea que el sistema componga.

Asignar método de inicio de sesión a usuarios y grupos de Active Directory

En la ficha **Doble verificación de acceso**, en la sección **Configuración de usuario**, aparece la lista de usuarios y grupos agregados a su sistema XProtect.

1. En el **método de inicio de sesión** columna, seleccione entre no inicio de sesión, no Doble verificación de acceso o método de entrega de códigos.
2. En el campo **Detalles**, añadir los detalles de entrega como direcciones de correo electrónico de usuarios individuales. La próxima vez que el usuario inicie sesión en XProtect Web Client o en la aplicación Milestone Mobile, se le pedirá un inicio de sesión secundario.
3. Si un grupo está configurado en Active Directory, el servidor Mobile utiliza detalles, como direcciones de correo electrónico, de Active Directory.

   Los grupos de Windows no admiten la Doble verificación de acceso.
4. Guardar la configuración.

Ha completado los pasos para configurar los usuarios para la Doble verificación de acceso por correo electrónico.

Acciones (explicadas)

Puede gestionar la disponibilidad de la ficha **Acciones** en el cliente Milestone Mobile activando o desactivando esto en la pestaña **General**. Acciones son por defecto activada, y se muestran aquí todas las acciones disponibles para los dispositivos conectados.

Nombrar una salida para usar en Milestone Mobile (explicado)

Con el fin de conseguir acciones que se muestran correctamente junto con la cámara actual, es importante que la salida utiliza exactamente el mismo nombre que la cámara.

Ejemplo:

Si usted tiene una cámara llamada "AXIS P3301, P3304 - 10. 100. 50. 110 - Cámara 1", también debe nombrar la acción "AXIS P3301, P3304 - 10. 100. 50. 110 - Cámara 1".

Puede añadir una descripción adicional al título después, por ejemplo, "AAXIS P3301,P3304 - 10.100.50.110 - Cámara 1 - Interruptor de la luz".

Importante: Si no se siguen estas convenciones de nombres, las acciones no están disponibles en la lista de acciones para la visión de la cámara asociada. En cambio, las acciones aparecen en la lista de otras acciones en la pestaña **acciones**.

Configuración del servidor Mobile

General

En la siguiente tabla se describen los ajustes de esta ficha.

General

Nombre	Descripción
Nombre del servidor	Introduzca un nombre del servidor Milestone Mobile.
Descripción	Introduzca una descripción opcional del servidor Milestone Mobile.
Servidor Mobile	Elige entre todos los servidores Milestone Mobile instalados actualmente en el sistema específico. Sólo los servidores Milestone Mobile que se ejecutan aparecen en la lista.
Método de acceso	Seleccione el método de autenticación que se utilizará cuando los usuarios accedan al servidor. Puede elegir entre: • **Automático** • **Autenticación de Windows** • **Autentificación básica**

Características

En esta sección, controla la disponibilidad de las características de Milestone Mobile.

Nombre	Descripción
Habilitar XProtect Web Client	Habilitar el acceso a XProtect Web Client. Esta característica está habilitada por defecto.
Activar todas las cámaras de visión	Incluya vista **Todas las cámaras**. Esta vista muestra todas las cámaras que un usuario puede ver en un servidor de grabación. Esta característica está habilitada por defecto.
Habilitar acciones (salidas y eventos)	Habilitar el acceso a acciones en Milestone Mobile clientes y XProtect Web Client. Esta característica está habilitada por defecto. Si desactiva esta función, los usuarios de cliente no podrán ver la salida y los eventos aunque estén configurados correctamente.

Nombre	Descripción
Habilitar fotogramas clave	Transmitir sólo fotogramas clave cuando los usuarios transmiten vídeo en dispositivos móviles y en XProtect Web Client. Esto usa menos ancho de banda.
Denegar el acceso del cometido Administrador incorporado al servidor Milestone Mobile	Habilite esto para excluir a los usuarios asignados al cometido de administrador incorporada de acceder al vídeo en clientes Milestone Mobile y XProtect Web Client.

Registrar configuración

Puede especificar si desea que el servidor Mobile Server cree archivos de registro para cambios de estado y desconexiones, por ejemplo, y cómo almacenarlos. La información está destinada principalmente a fines de depuración.

Nombre	Descripción
Habilitado	Activar o desactivar el registro de las acciones del cliente Milestone Mobile en un archivo de registro separado.
Ingrese la ubicación del archivo	Especifique dónde el sistema guarda los archivos de registro.
Mantener los registros de	Especifique el número de días para mantener los registros (el valor predeterminado es de tres días).

Configuración de copia de seguridad

Si su sistema tiene varios servidores Mobile Server, puede utilizar la función de copia de seguridad para exportar los valores actuales e importarlos en otros servidores Mobile Server.

Nombre	Descripción
Importar	Importe un archivo XML con una nueva configuración de servidor Milestone Mobile.
Exportación	Exporte su configuración de servidor Milestone Mobile. El sistema almacena la configuración en un archivo XML.

Conectividad

Los ajustes de la ficha **Conectividad** se utilizan en las tareas siguientes:

- Configurar los ajustes de conexión.
- Enviar un mensaje de correo electrónico para ayudar a los usuarios conectar su dispositivo móvil para Milestone Mobile servidores.
- Habilitar conexiones con Milestone Mobile servidores en una red compleja.

Para obtener descripciones paso a paso de estas tareas, consulte Configurar Smart Connect (ver "Puesta en funcionamiento de Smart Connect" en la página 389).

General

Nombre	Descripción
Tipo de conección	Elige cómo los clientes deben conectarse al servidor Milestone Mobile. Se puede elegir entre las siguientes opciones: **Sólo HTTP**, **HTTP y HTTPS** o **Sólo HTTPS**. **Nota:** Si selecciona **sólo HTTPS**, los dispositivos que ejecutan Windows Phone, sólo pueden conectarse si dispone de un certificado de una autoridad de certificación (CA) instalada en su servidor Milestone Mobile. Cuestión entidades emisoras de certificados digitales que verifican las identidades de los usuarios y los sitios web que intercambian datos a través de Internet. Ejemplos de entidades emisoras son empresas como Comodo, Symantec, y GoDaddy. Antes de encender conexiones seguras, asegúrese de que está familiarizado con los certificados digitales. Para aprender a añadir un certificado de servidor de Milestone Mobile, ver editar certificados (ver "Editar certificado" en la página *409*).
Tiempo de espera del cliente (HTTP)	Establecer un marco de tiempo para la frecuencia del cliente Milestone Mobile debe indicar al servidor Mobile que está en funcionamiento. El valor predeterminado es de 30 segundos. Milestone recomienda que usted **no** haga aumente el marco de tiempo.
Habilitar la capacidad de detección de UPnP	Esto hace que el servidor Mobile Server sea detectable en la red mediante los protocolos UPnP. Los clientes Mobile Server tienen funcionalidad de exploración para encontrar servidores Mobile Server basados en UPnP.
Habilitar la asignación automática de puertos	Cuando el servidor Mobile Server se instala detrás del cortafuegos, se requiere una asignación de puertos en el enrutador, por lo que los clientes pueden seguir accediendo al servidor desde Internet. La opción **Habilitar la asignación automática de puertos** permite que el servidor Mobile Server realice esta asignación de puertos por sí mismo siempre que el enrutador esté configurado para ello.
Habilitar Smart Connect	Smart Connect le permite verificar que ha configurado correctamente el servidor Mobile Server sin iniciar sesión con un dispositivo móvil o una tableta para realizar la validación. También simplifica el proceso de conexión para los usuarios del cliente.

Acceso a Internet

Nombre	Descripción
Configurar acceso a Internet personalizado	Si utiliza la asignación de puertos UPnP, a conexiones directas a una conexión específica, seleccione la casilla de verificación **configurar el acceso a Internet a medida**. A continuación, proporcione la **dirección IP** o **nombre de host** y el puerto que se utilizará para la conexión. Por ejemplo, puede hacerlo si su router no es compatible con UPnP, o si tiene una cadena de routers.
Seleccionar para recuperar dinámicamente la dirección IP	Si sus direcciones IP a menudo cambian, seleccione la casilla de verificación **Seleccionar para recuperar la dirección IP dinámicamente** .

Nombre	Descripción
Direcciones descubiertas automáticamente	Muestra las direcciones IP de este Mobile Server que el sistema ha descubierto por sí mismo.

Notificación de Smart Connect

Nombre	Descripción
Invitación por correo electrónico a	Introduzca la dirección de correo electrónico del destinatario de la notificación de Smart Connect.
Idioma del correo electrónico	Especifique el idioma utilizado en el correo electrónico.
Token de conexión inteligente	Un identificador único que los usuarios de dispositivos móviles pueden usar para conectarse al servidor Mobile Server.
Enlace a Smart Connect	Un enlace que los usuarios de dispositivos móviles pueden usar para conectarse al servidor Mobile Server.

Estado de servidor

Ver los detalles del estado de su servidor Mobile. Los detalles son de sólo lectura:

Nombre	Descripción
Servidor activo desde	Muestra el tiempo que el servidor de Mobile ha estado funcionando desde que fue detenida la última vez.
Uso del procesador	Muestra el uso actual de la CPU en el servidor Mobile.
Ancho de banda externa	Muestra el ancho de banda actual en uso entre los dispositivos móviles y el servidor Mobile.

Usuarios activos

Consulte los detalles de estado de los dispositivos móviles conectados a su servidor Mobile.

Nombre	Descripción
Nombre de usuario	Muestra el nombre de usuario para cada usuario de cliente Mobile conectado al servidor Mobile.
Estado	Muestra la relación actual entre el servidor Mobile y el usuario cliente Mobile Server en cuestión. Los estados posibles son: • **Conectado**: Un estado previo a los servidores de intercambio de claves y cifrado de credenciales. • **Conectado**; El usuario de cliente Mobile está conectado al sistema XProtect.
Uso de ancho de banda (kB/s)	Muestra el nivel de ancho de banda utilizado por el usuario de cliente Mobile en cuestión.

Nombre	Descripción
Secuencias transcodificadas	Muestra el número de secuencias de vídeo transcodificadas actualmente abiertas para cada usuario de cliente Mobile.

Rendimiento

En la ficha **rendimiento**, se pueden establecer las siguientes limitaciones en el rendimiento del servidor Milestone Mobile:

Configuración

Nombre	Descripción
Activar imágenes a tamaño completo	Habilite el servidor Milestone Mobile para enviar imágenes de tamaño completo a los clientes Milestone Mobile o XProtect Web Client. Habilitar imágenes de tamaño completo utiliza más ancho de banda. Además, habilitar esta opción inhabilita todas las reglas establecidas en los niveles **de limitaciones de flujo de vídeo** que se describen a continuación.
Limitar los flujos de reproducción	Habilite y especifique el número máximo de secuencias de vídeo de reproducción actualmente abiertas para el usuario de cliente Mobile relevante.

Niveles de limitaciones de flujo de vídeo

Nivel 1

El nivel 1 es el límite predeterminado colocado en el servidor Milestone Mobile. A menos que haya habilitado el envío de imágenes de tamaño completo arriba, cualquier limitación que establezca aquí siempre se aplicará al flujo de video de Milestone Mobile.

Nombre	Descripción
Nivel 1	Seleccione la casilla de verificación para activar el primer nivel de limitaciones al rendimiento del servidor Milestone Mobile.
Max FPS	Establecer un límite para el número máximo de fotogramas por segundo (FPS) para enviar desde el servidor Milestone Mobile a los clientes.
Resolución máxima de imagen	Establecer un límite para la resolución de imagen para enviar desde el servidor Milestone Mobile a los clientes.

Nivel 2

Si prefiere imponer un nivel diferente de limitaciones que el predeterminado en **Nivel 1**, puede seleccionar la casilla de verificación **Nivel 2** en su lugar. No se puede establecer ninguna configuración más altos que lo que les ha fijado en el primer nivel. Si, por ejemplo, establecer el máximo de FPS a 45 en el **Nivel 1**, se puede establecer el máximo de FPS **Nivel 2** sólo para 44 o por debajo.

Nombre	Descripción
Nivel 2	Seleccione la casilla de verificación para activar el segundo nivel de limitaciones al rendimiento del servidor Milestone Mobile.
Umbral de la CPU	Establecer un umbral para la carga de la CPU en el servidor Milestone Mobile antes de que el sistema impone limitaciones de flujo de vídeo.
Límite de ancho de banda	Establecer un umbral de carga de ancho de banda en el servidor Milestone Mobile antes de que el sistema impone limitaciones de flujo de vídeo.
Max FPS	Establecer un límite para el número máximo de fotogramas por segundo (FPS) para enviar desde el servidor Milestone Mobile a los clientes.
Resolución máxima de imagen	Establecer un límite para la resolución de imagen para enviar desde el servidor Milestone Mobile a los clientes.

Nivel 3

También puede seleccionar una casilla de verificación **Nivel 3** para crear un tercer nivel para las limitaciones. No se puede establecer ninguna configuración más alta que lo que les ha fijado en el **nivel 1** y **Nivel 2**. Si, por ejemplo, establecer el **Max FPS** a 45 sobre **Nivel 1** y 32 para nivelar el **nivel 2**, se puede establecer el **Max FPS** el **nivel 3** sólo para 31 o por debajo.

Nombre	Descripción
Nivel 3	Active la casilla de verificación para habilitar el tercer nivel de limitaciones para el rendimiento del servidor Milestone Mobile.
Umbral de la CPU	Establecer un umbral para la carga de la CPU en el servidor Milestone Mobile antes de que el sistema impone limitaciones de flujo de vídeo.
Límite de ancho de banda	Establecer un umbral de carga de ancho de banda en el servidor Milestone Mobile antes de que el sistema impone limitaciones de flujo de vídeo.
Max FPS	Establecer un límite para los cuadros por segundo (FPS) para enviar desde el servidor Milestone Mobile a los clientes.
Resolución máxima de imagen	Establecer un límite para la resolución de imagen para enviar desde el servidor Milestone Mobile a los clientes.

El sistema no se enciende al instante de un nivel a otro nivel. Si la CPU o el umbral de ancho de banda va de menos del cinco por ciento por encima o por debajo de los niveles indicados, el nivel actual se mantiene en uso.

Tenga en cuenta que si se habilita **Activar imágenes a tamaño completo** en la ficha **general**, se aplica ninguna de las **Rendimiento** niveles.

Investigaciones

Configuración de las investigaciones

Puede habilitar las investigaciones para que las personas puedan usar XProtect Web Client y Milestone Mobile para acceder al video grabado e investigar incidentes, y preparar y descargar evidencia de video.

Nombre	Descripción
Carpeta de investigaciones	Especificar dónde almacenar vídeo para investigaciones.
Limitar el tamaño de la carpeta de investigaciones a	Introduzca el número máximo de megabytes que la carpeta de investigaciones puede contener. El tamaño predeterminado es 2000 MB.
Ver investigaciones realizadas por otros usuarios	Seleccione esta casilla para permitir a los usuarios acceder a las investigaciones que ellos no crean.
Incluir marcas de tiempo para las exportaciones AVI	Seleccione esta casilla de verificación para incluir la fecha y hora en que el archivo AVI se descargó.
Códec utilizado para la exportación AVI	Seleccione el formato de compresión que se utilizará en la preparación de paquetes de AVI para su descarga. Los códecs que puede elegir pueden ser diferentes, dependiendo de su sistema operativo. Si no ve el códec que desee, puede añadirlo a la lista de instalarlo en el equipo en el servidor Milestone Mobile se está ejecutando.
Mantenga o borre datos cuando las exportaciones fallen (MKV y AVI)	Seleccione si desea conservar los datos que no estaba preparado correctamente para su descarga en una investigación, o eliminarlo.

Investigaciones

Nombre	Descripción
Investigaciones	Enumera las investigaciones que se han realizado hasta ahora en el sistema. Utilice el **Borrar** o **Borrar todos** los botones si ya no desea seguir una investigación. Esto puede ser útil si, por ejemplo, desea hacer más espacio en disco disponible en el servidor.
Detalles de la investigación	Para eliminar archivos de vídeo individuales que se exportaron a cabo una investigación, pero manteniendo la investigación, seleccione la investigación en la lista. En el **Detalles de la investigación** grupo, haga clic en el icono de eliminar a la derecha de la **base de datos**, **AVI**, o **MKV** campos para las exportaciones.

Vídeo push

Se pueden especificar los siguientes ajustes si se habilita empuje del vídeo:

Nombre	Descripción
Vídeo Push	Activar inserción de vídeo en el servidor Mobile.
Número de canales	Muestra el número de canales de inserción de video activados en su sistema XProtect.
Canal	Muestra el número de canal para el canal correspondiente. No editable.
Puerto	Número de puerto para el canal de vídeo de empuje relevante.
Dirección MAC	Dirección MAC para el canal de vídeo de empuje relevante.

Nombre	Descripción
Nombre de usuario	Introduzca el nombre de usuario asociado con el canal de empuje de vídeo correspondiente.
Nombre cámara	Muestra el nombre de la cámara si la cámara ha sido identificada.

Una vez que haya completado todos los pasos necesarios (ver "Configurar empuje video para transmitir vídeo" en la página 394), haga clic en **Buscar cámaras** para buscar la cámara correspondiente.

Notificaciones

Utilice la pestaña **Notificaciones** para activar o desactivar las notificaciones del sistema y las notificaciones push.

Si activa las notificaciones, y ha configurado una o más alarmas y eventos, Milestone Mobile notifica a los usuarios cuando se produce un evento. Cuando la aplicación está abierta, las notificaciones se entregan en Milestone Mobile en el dispositivo móvil. Notificaciones push notificar a los usuarios que no tienen abierto el Milestone Mobile. Estas notificaciones se envían al dispositivo móvil.

Para obtener más información, consulte Configurar notificaciones de envío a dispositivos móviles (ver "Configurar el envío de notificaciones a dispositivos móviles" en la página 392).

En la siguiente tabla se describen los ajustes de esta ficha.

Nombre	Descripción
Notificaciones	Seleccione esta casilla de verificación para activar las notificaciones.
Mantener el registro del dispositivo	Seleccione esta casilla de verificación para almacenar información sobre los dispositivos y usuarios que se conectan a este servidor. El sistema envía notificaciones a estos dispositivos. Si desactiva esta casilla de verificación, también se borra la lista de dispositivos. Para que los usuarios comienzan a recibir las notificaciones de nuevo, se debe seleccionar la casilla de verificación, y los usuarios deben conectar sus dispositivos al servidor de nuevo.

Dispositivos registrados

Nombre	Descripción
Habilitado	Seleccione esta casilla de verificación para comenzar a enviar notificaciones al dispositivo.
Nombre de dispositivo	Una lista de los dispositivos móviles que se han conectado a este servidor. Puede iniciar o detener el envío de notificaciones a dispositivos específicos seleccionando o desactivando la casilla de verificación **habilitada**.
Usuario	Nombre del usuario que recibirá notificaciones.

Doble verificación de acceso

Funcionalidad disponible depende del sistema que está utilizando. Ver tabla de comparación de productos (en la página 24) para más información.

Utilice la ficha **Doble verificación de acceso** para habilitar y especificar un paso de inicio de sesión adicional para los usuarios de la aplicación Milestone Mobile en sus dispositivos móviles iOS, Windows Phone o Android o XProtect Web Client.

El primer tipo es la contraseña y el segundo tipo, el código de verificación, que puede configurar para ser enviado por correo electrónico al usuario.

Para obtener más información, consulte Configurar usuarios para la Doble verificación de acceso (ver "Configurar usuarios para la Doble verificación de acceso por correo electrónico" en la página 396).

Las siguientes tablas describen los ajustes de esta pestaña.

Configuración del proveedor > **Correo electrónico**

Nombre	Descripción
Servidor SMTP	Introduzca la dirección IP o el nombre de host del servidor de protocolo de transferencia de correo (SMTP) simple para los correos electrónicos de Doble verificación de acceso.
Puerto del servidor SMTP	Especifique el puerto del servidor SMTP para enviar correos electrónicos. El número de puerto predeterminado es 25 sin SSL y 465 con SSL.
Usar SSL	Seleccione esta casilla de verificación si su servidor SMTP admite el cifrado SSL.
Nombre de usuario	Especifique el nombre de usuario para iniciar sesión en el servidor SMTP.
Contraseña	Especifique la contraseña para iniciar sesión en el servidor SMTP.
Utilice autenticación de contraseña segura (SPA)	Seleccione esta casilla de verificación si su servidor SMTP admite SPA.
Dirección de correo electrónico del remitente	Especifique la dirección de correo electrónico para enviar los códigos de verificación.
Asunto del email	Especifique el título del asunto para el correo electrónico. Ejemplo: Su código de Doble verificación de acceso.
Texto del correo electrónico	Escriba el mensaje que desea enviar. Ejemplo: Su código es {0}. Si olvida incluir la variable **{0}**, el código se agrega al final del texto de forma predeterminada.

Configuración del código de verificación

Nombre	Descripción
Tiempo de espera de reconexión (0-30 minutos)	Especifique el período dentro del cual los usuarios de cliente Mobile no tienen que reverificar su inicio de sesión en caso de, por ejemplo, una red desconectada. El período predeterminado es de 3 minutos. Esta configuración no es válida para XProtect Web Client.

Nombre	Descripción
El código caduco después de (1-10 minutos)	Especifique el período dentro del cual el usuario puede utilizar el código de verificación recibido. Después de este período, el código no es válido y el usuario tiene que solicitar un nuevo código. El período predeterminado es de 5 minutos.
Intentos de entrada de código (1-10 intentos)	Especifique el número máximo de intentos de entrada de código antes de bloquear el usuario. El número predeterminado es 3.
Longitud del código (4-6 caracteres)	Especifique el número de caracteres para el código. La longitud predeterminada es 6.
Composición del código	Especifique la complejidad del código que desea que el sistema componga. Puede seleccionar entre: • **Mayúsculas latinas (A-Z)** • **Latín minúsculas (a-z)** • **Dígitos (0-9)** • **Caracteres especiales (!@#...)**

Configuración del usuario

Nombre	Descripción
Usuarios y grupos	Lista los usuarios y grupos agregados al sistema XProtect. Si un grupo está configurado en Active Directory, el servidor Mobile utiliza detalles, como direcciones de correo electrónico, de Active Directory. Los grupos de Windows no admiten la Doble verificación de acceso.
Método de verificación	Seleccione una configuración de verificación para cada usuario o grupo. Puede seleccionar entre: • **Sin iniciar sesión**: el usuario no puede iniciar sesión. • **No hay Doble verificación de acceso:** el usuario debe introducir el nombre de usuario y la contraseña. • **Correo electrónico**: el usuario debe introducir un código de verificación además del nombre de usuario y la contraseña.
Detalles de usuario	Escriba la dirección de correo electrónico a la que cada usuario recibirá los códigos.

Mobile Server Manager

Administrador de servidores móviles (explicado)

El Mobile Server Manager es una característica bandeja controlado conectado al servidor de Mobile. Clic derecho en el icono del Mobile Server Manager en la bandeja del sistema se abre un menú desde donde se puede acceder fácilmente a la funcionalidad del servidor Mobile.

Puede realizar las siguientes acciones:

- Abrir XProtect Web Client (ver "Acceder a XProtect Web Client" en la página 408)
- Iniciar, detener y reiniciar el servicio Mobile (ver "Inicie, detenga y reinicie el servicio Mobile Server" en la página 411)
- Rellene o cambiar las credenciales del servidor de vigilancia (ver "Rellene / editar las credenciales del servidor de vigilancia" en la página 411)
- Mostrar/editar números de puerto (en la página 411)
- Editar certificado (en la página 409)
- Abra el archivo de registro de hoy (ver "Acceso a registros e investigaciones (explicado)" en la página 409)
- Abrir carpeta de registro (ver "Acceso a registros e investigaciones (explicado)" en la página 409)
- Abrir carpeta de investigaciones (ver "Acceso a registros e investigaciones (explicado)" en la página 409)
- Mostrar el estado del servidor Mobile (ver "Mostrar estado (explicado)" en la página 409)

Acceder a XProtect Web Client

Si tiene un servidor Milestone Mobile instalado en su computadora, puede usar XProtect Web Client para acceder a sus cámaras y vistas. Como no necesita instalar XProtect Web Client, puede acceder a él desde la computadora donde instaló el servidor Milestone Mobile o cualquier otra computadora que desee utilizar para este fin.

1. Configure el servidor Milestone Mobile en Management Client.
2. Si está utilizando la computadora donde está instalado el servidor Milestone Mobile, puede hacer clic con el botón derecho en el ícono del Mobile Server Manager en la bandeja del sistema y seleccionar **Abrir XProtect Web Client**.
3. Si no está utilizando el equipo donde está instalado el servidor de Milestone Mobile, se puede acceder a él desde un navegador. Continúe con el paso 4 en este proceso.
4. Abra un navegador de Internet (Internet Explorer, Mozilla Firefox, Google Chrome o Safari).
5. Escriba la dirección IP externa, es decir, la dirección externa y el puerto del servidor en el que se ejecuta el servidor Milestone Mobile.

   Ejemplo: El servidor Milestone Mobile se instala en un servidor con dirección IP 127.2.3.4 y se configura para aceptar conexiones HTTP en el puerto 8081 y conexiones HTTPS en el puerto 8082 (la configuración predeterminada del instalador).

En la barra de direcciones de su navegador, escriba: http://1.2.3.4:8081 si desea utilizar una conexión HTTP estándar o https://1.2.3.4:8082 para usar una conexión segura HTTPS. Ahora ya puede comenzar a usar XProtect Web Client.

6. Añada la dirección como un marcador en su navegador para un fácil acceso futuro a XProtect Web Client. Si utiliza XProtect Web Client en el equipo local en el que instaló el servidor Milestone Mobile, también puede utilizar el acceso directo del escritorio que crea el instalador. Haga clic en el acceso directo para iniciar el navegador predeterminado y abra XProtect Web Client.

Debe eliminar la caché de los exploradores de Internet que ejecutan XProtect Web Client antes de poder utilizar una nueva versión de XProtect Web Client. Los administradores del sistema deben solicitar a sus usuarios de XProtect Web Client que borren su caché del navegador después de la actualización, o fuercen esta acción de forma remota (puede realizar esta acción solo en Internet Explorer en un dominio).

Mostrar estado (explicado)

Haga clic con el botón secundario en el icono de Mobile Server Manager y seleccione **Mostrar estado** o haga doble clic en el icono de Mobile Server Manager para abrir una ventana que muestre el estado del servidor Mobile. Se puede ver la siguiente información:

Nombre	Descripción
Servidor en funcionamiento desde	Hora y fecha del momento en que el servidor de Mobile se inició el pasado.
Usuarios conectados	Número de usuarios conectados actualmente al servidor Mobile.
Decodificación de hardware	Indica si la descodificación acelerada por hardware está en acción en el servidor Mobile.
Uso de CPU	¿Cuántas% de la CPU está siendo utilizado por el servidor Mobile.
El historial de uso de la CPU	Un gráfico que detalla la historia de uso de la CPU por el servidor Mobile.

Acceso a registros e investigaciones (explicado)

Mobile Server Manager le permite acceder rápidamente al archivo de registro del día, abrir la carpeta a la que se guardan los archivos de registro y abrir la carpeta a la que se guardan las investigaciones.

Para abrir cualquiera de estos, haga clic con el botón secundario en el Mobile Server Manager y seleccione **Abrir el archivo de registro de hoy**, **Abrir carpeta de registro** o **Abrir carpeta de investigación** respectivamente **.**

Importante: Si desinstala Milestone Mobile de su sistema, no se eliminan los archivos de registro. Los administradores con los derechos adecuados pueden acceder a estos archivos de registro en un contador de tiempo más tarde, o decidir eliminarlos si no se necesitan más. La ubicación predeterminada de los archivos de registro se encuentra en la carpeta **ProgramData**. Si cambia la ubicación predeterminada de los archivos de registro, los registros existentes no se copian en la nueva ubicación ni tampoco se eliminan.

Editar certificado

Si desea utilizar un protocolo HTTPS seguro para establecer la conexión entre un servidor Milestone Mobile y los dispositivos móviles o XProtect Web Client, debe aplicar un certificado válido en el servidor. El certificado confirma que el titular del certificado está autorizado a establecer conexiones seguras.

- Si ejecuta una instalación **Único equipo**, el servidor Milestone Mobile se instala en silencio y el sistema no crea un certificado.Puede crear una como se explica más abajo.

- Si ejecuta una instalación **Típica**, el sistema genera un certificado autofirmado al instalar el servidor Milestone Mobile.Puede cambiar a un certificado emitido por otro sitio de confianza, ver más abajo.
- Si ejecuta una instalación **Personalizada**, puede elegir entre generar un certificado autofirmado o cargar un archivo que contiene un certificado emitido por otro sitio de confianza.

Certificados de CA

Los certificados emitidos por CA (Autoridad de certificación) tienen una cadena de certificados y en la raíz de esa cadena se encuentra el certificado raíz de CA. Cuando un dispositivo o navegador ve este certificado, compara su certificado raíz con los preinstalados en el sistema operativo (Android, iOS, Windows, etc.).Si el certificado raíz aparece en la lista de certificados preinstalados, el sistema operativo garantizará al usuario que la conexión con el servidor es lo suficientemente segura.Estos certificados se emiten para un nombre de dominio y no son gratuitos.

Certificados autofirmados

Cualquiera puede crear certificados autofirmados.No tienen un certificado raíz de CA y los sistemas operativos lo consideran menos seguro.Proporcionan seguridad para ataques simples, pero hay algunas situaciones en las que no garantizan la seguridad de la conexión.La facilidad de los certificados autofirmados es que el servidor Milestone Mobile puede crearlos y son gratuitos.

Nota: Si desea utilizar conexiones seguras (HTTPS), los dispositivos que ejecutan iOS 9.0 o posterior, o Windows Phone, sólo pueden conectarse si dispone de un certificado de una autoridad de certificación (CA) instalada en su servidor Milestone Mobile. Cuestión entidades emisoras de certificados digitales que verifican las identidades de los usuarios y los sitios web que intercambian datos a través de Internet. Ejemplos de entidades emisoras son empresas como Comodo, Symantec, y GoDaddy. Antes de encender conexiones seguras, asegúrese de que está familiarizado con los certificados digitales.

Si desea crear o cambiar un certificado, haga lo siguiente:

1. En una computadora con Management Client instalado, haga clic con el botón derecho en el icono del Mobile Server Manager en la bandeja del sistema y seleccione **Modificar certificado**.
2. Elige uno de los siguientes:
   - Generar un certificado autofirmado.
   - Cargar un archivo de certificado de CA.

Generar un certificado autofirmado

1. Seleccione el opción **Generar un certificado auto-firmado** y haga clic en **OK**.
2. Espere unos segundos mientras el sistema se instala el certificado.
3. Cuando haya terminado, se abre una ventana y le informa de que el certificado se ha instalado correctamente.

   El servicio Mobile Server se reinicia para aplicar el cambio.

Localizar un archivo de certificado de CA

1. Seleccione el **Cargar un archivo de certificado** opción.
2. Rellene la ruta para el archivo de certificado o haga clic en el cuadro ... para abrir una ventana donde se puede buscar el archivo.

3. Rellene la contraseña conectado al archivo de certificado.
4. Cuando haya terminado, haga clic en **Aceptar**.

   El usuario del cliente Mobile será invitado a aceptar una vez más el certificado, si no es un problema de CA.

Rellene / editar las credenciales del servidor de vigilancia

1. En una computadora con Management Client instalado, haga clic con el botón derecho en el icono MobileServer Manager y seleccione **Credenciales de servidor de vigilancia**.
2. Rellene la **Dirección URL del servidor**.
3. Seleccionar qué usuario que desea iniciar la sesión como:
   - Administrador del sistema local (no se necesitan credenciales) o
   - Una cuenta de usuario especificada (credenciales necesarias).
4. Si ha elegido una cuenta de usuario especificada, rellene **Nombre de usuario** y **Contraseña**.
5. Cuando haya terminado, haga clic en **Aceptar**.

Mostrar/editar números de puerto

1. En una computadora con Management Client instalado, haga clic con el botón derecho en el icono del Administrador del servidor móvil y seleccione **Mostar/Modificar los números de puertos**.
2. Para modificar los números de puerto, escriba el número de puerto correspondiente. Puede indicar un número de puerto estándar para las conexiones HTTP y / o un número de puerto seguro para las conexiones HTTPS.
3. Cuando haya terminado, haga clic en **Aceptar**.

Inicie, detenga y reinicie el servicio Mobile Server

Si es necesario, puede iniciar, detener y reiniciar el servicio Mobile desde el Mobile Server Manager.

- Para realizar cualquiera de estas tareas, haga clic con el botón derecho en el icono del Administrador del servidor móvil y seleccione **servicio Start Mobile**, **servicio Stop Mobile Server**o **servicio Restart Mobile Server** respectivamente**.**

Solución de problemas Milestone Mobile

Conexiones

1. **¿Por qué no me puedo conectar a mi cliente Milestone Mobile a mis grabaciones / servidor Milestone Mobile?**

   Con el fin de conectarse a las grabaciones, el servidor Milestone Mobile debe estar instalado en el servidor que ejecuta el sistema XProtect o, alternativamente, en un servidor dedicado. También son necesarios los ajustes Milestone Mobile relevante en la configuración de gestión de vídeo XProtect. Estos se instalan ya sea como plug-ins o como parte de una instalación o actualización del producto. Para más detalles sobre cómo obtener el servidor Milestone Mobile y cómo integrar los ajustes en su

sistema XProtect relacionados con el cliente Milestone Mobile, consulte la sección de configuración (ver "Configuración Milestone Mobile" en la página 389).

2. **Acabo de encender mi firewall, y ahora no puedo conectar un dispositivo móvil a mi servidor. ¿Por qué no?**

   Si el servidor de seguridad se apaga mientras que ha instalado el servidor Milestone Mobile, debe habilitar manualmente TCP y UDP comunicaciones.

3. **¿Cómo evitar la advertencia de seguridad cuando ejecuto XProtect Web Client a través de una conexión HTTPS?**

   La advertencia aparece porque la información de la dirección del servidor en el certificado es incorrecta. Todavía será encriptada la conexión.
   El certificado autofirmado en el servidor de Milestone Mobile necesita ser reemplazado con su propio certificado coincide con la dirección del servidor utilizado para conectarse al servidor de Milestone Mobile. Estos certificados se obtienen a través de las autoridades oficiales de firma de certificados como Verisign. Consulte a la autoridad de firma escogida para más detalles.
   Servidor Milestone Mobile no utiliza Microsoft IIS. Esto significa que las instrucciones proporcionadas para la generación de archivos de firma de certificados petición (RSC) por la autoridad de firmas utilizando el IIS no es aplicable para el servidor Milestone Mobile. Debe crear manualmente RSE-archivo usando herramientas de línea de comandos de certificados u otra aplicación similar de otro fabricante. Tenga en cuenta que este proceso debe ser realizado por los administradores de sistemas y usuarios avanzados.

Calidad de la imagen

1. **¿Por qué a veces es la calidad de imagen pobre cuando puedo ver el vídeo en el cliente Milestone Mobile?**

   El servidor Milestone Mobile ajusta automáticamente la calidad de imagen de acuerdo con el ancho de banda disponible entre el servidor y el cliente. Si experimenta una calidad de imagen inferior a la del XProtect® Smart Client, es posible que tenga poco ancho de banda para obtener imágenes de resolución completa a través del cliente Milestone Mobile. La razón de esto puede ser demasiado poco ancho de banda ascendente desde el servidor o muy poco ancho de banda aguas abajo en el cliente. Ver el **XProtect Smart Client Manual del usuario** cual se puede descargar desde nuestro sitio web (http://www.milestonesys.com/support/manuals-and-guides/).

   Si se encuentra en una zona con un ancho de banda inalámbrica mixta, puede observar que la calidad de la imagen mejora cuando se introduce un área con mejor ancho de banda.

2. **¿Por qué es la calidad de imagen pobre cuando me conecto a mi sistema de gestión de vídeo XProtect en el hogar a través de Wi-Fi en mi oficina?**

   Compruebe su ancho de banda de Internet en casa. Muchas conexiones de internet privadas tienen diferentes anchos de banda de carga y descarga a menudo descritos como, por ejemplo, 20 Mbit / 2 Mbit. Esto se debe a que los usuarios domésticos no suelen necesitar para cargar grandes cantidades de datos a Internet, pero consumen una gran cantidad de datos en su lugar. El sistema de gestión de vídeo XProtect necesita para enviar vídeo al cliente Milestone Mobile y está limitada por la velocidad de subida de su conexión. Si la calidad de imagen baja es consistente en múltiples lugares en los que la velocidad de descarga de la red del cliente Milestone Mobile es buena, el problema puede ser resuelto mediante la mejora de la velocidad de subida de su conexión a Internet en casa.

Descodificación acelerada por hardware

1. **¿Tiene mi apoyo procesador de hardware-acelerada de decodificación?**

Sólo los nuevos procesadores de Intel soporte de hardware de descodificación acelerada. Compruebe sitio web de Intel (http://ark.intel.com/search/advanced?s=t&MarketSegment=DT&QuickSyncVideo=true) si es compatible con su procesador.

En el menú, asegúrese de **Tecnologías** > **Intel Quick Sync Video** se establece en **Sí**.

Si se admite el procesador, la descodificación acelerada por hardware está activada por defecto. Puede ver el estado actual en **Mostrar estado** en el Administrador de servidor Mobile (ver "Mostrar estado (explicado)" en la página 409).

2. **¿Tiene mi apoyo al sistema operativo del hardware-acelerada de decodificación?**

   Sólo para Windows 8 y Windows Server 2012 o posterior son compatibles.

   Asegúrese de instalar los controladores gráficos más recientes desde el sitio web de Intel en su sistema. Estos controladores no están disponibles en Windows Update.

   No se admite la aceleración por hardware de descodificación, si el servidor Mobile está instalado en un entorno virtual.

3. **¿Cómo desactivo la decodificación acelerada por hardware en el servidor Mobilel? (Avanzado)**

   Si el procesador en el servidor Mobile soporta la decodificación acelerada por hardware, que es activado por defecto. Para activar la descodificación acelerada por hardware apagado, haga lo siguiente:

   1. Busque el archivo VideoOS.MobileServer.Service.exe.config. La ruta de acceso es normalmente: C:\Program Files\Milestone\Milestone Mobile Server\VideoOS.MobileServer.Service.exe.config.
   2. Abra el archivo en el Bloc de notas o un editor de texto similar. Si es necesario, asociar el tipo de archivo .config con el Bloc de notas.
   3. Busque el campo <add key="HardwareDecodingMode" value="Auto" />.
   4. Reemplazar el valor de "Auto" a "Off".
   5. Guarde y cierre el archivo.

Milestone ONVIF Bridge

Acerca de Milestone ONVIF Bridge

ONVIF es un foro abierto, global que está trabajando para estandarizar y asegurar la forma en que los productos de video vigilancia IP se comunican. El objetivo es facilitar el intercambio de datos de vídeo. Por ejemplo, para permitir la aplicación de la ley, los centros de vigilancia, o de organizaciones similares para acceder rápidamente a flujos de vídeo en directo y grabados en cualquier sistema de vigilancia basado en IP.

Milestone Systems quiere apoyar este objetivo, y ha desarrollado la Milestone ONVIF Bridge hacia ese fin. Milestone ONVIF Bridge forma parte de la plataforma abierta Milestone y ofrece una interfaz que admite las partes del estándar ONVIF para recuperar vídeo en directo y grabado de cualquier producto Milestone VMS.

En este documento se proporciona la siguiente:

- Información sobre los enlaces ONVIF estándar y materiales de referencia.
- Instrucciones para instalar y configurar el Milestone ONVIF Bridge en su producto VMS XProtect.

- Ejemplos de cómo habilitar diferentes tipos de clientes ONVIF para transmitir vídeo en directo y grabado desde XProtect productos VMS.

Milestone ONVIF Bridge y el estándar ONVIF

El estándar ONVIF facilita el intercambio de información mediante la definición de un protocolo común. El protocolo contiene ONVIF perfiles, que son colecciones de ETI entre ONVIF dispositivos compatibles.

Milestone ONVIF Bridge es compatible con las partes del ONVIF Perfil G y Perfil S que proporcionan acceso a vídeo en directo y grabado, y la capacidad de controlar las cámaras de giro, inclinación y zoom:

- Perfil G - Proporciona soporte para grabación de vídeo, almacenamiento, búsqueda y recuperación. Para obtener más información, consulte ONVIF Perfil G Especificación (https://www.onvif.org/Portals/0/documents/specs/ONVIF_Profile_G_Specification_v1-0.pdf)
- Perfil S - Proporciona soporte para streaming de video en vivo usando el códec H.264, la transmisión de audio y controles de giro, inclinación y zoom (PTZ). Para obtener más información, consulte ONVIF Perfil S Especificaciones (http://www.onvif.org/Portals/0/documents/op/ONVIF_Profile_S_Specification_v1-1-1.pdf).

Para obtener más información sobre el estándar ONVIF, consulte la página web ONVIF® (http://www.onvif.org/).

Perfiles ONVIF apoyar "llegar" funciones que recuperan datos, y "ajustar" las funciones que configuran los ajustes. Cada función es obligatoria, condicionales u opcionales. Por razones de seguridad, Milestone ONVIF Bridge sólo admite las funciones obligatorias, condicionales y opcionales de "get" que hacen lo siguiente:

- Solicitud de vídeo
- Autenticar a los usuarios
- Flujo de vídeo
- Reproducir vídeo grabado

Acerca de los clientes ONVIF

Los clientes de ONVIF son aplicaciones informáticas o programas de software que utilizan ONVIF Webservices. Ejemplos de clientes ONVIF son servidores, reproductores de medios, sistemas de vigilancia basados en IP o puentes como el Milestone ONVIF Bridge.

El Real Time Streaming Protocol (RTSP) se utiliza para establecer y sesiones de medios de control entre dos o más puntos finales. El Milestone ONVIF Bridge utiliza ONVIF Profile S y RTSP para gestionar solicitudes de vídeo de un cliente ONVIF y para transmitir vídeo desde una instalación XProtect al cliente ONVIF.

Por defecto, la comunicación entre ONVIF clientes y el servidor ONVIF Bridge utiliza los siguientes puertos:

- ONVIF 580 puerto. ONVIF clientes utilizan este puerto para presentar solicitudes de flujos de vídeo
- RTSP puerto 554. Milestone ONVIF Bridge utiliza este puerto para transmitir vídeo a clientes ONVIF

ONVIF clientes pueden acceder al puerto RTSP en el Milestone ONVIF Bridge directamente. Por ejemplo, el reproductor multimedia VLC o un plug-in VLC en un navegador puede recuperar y visualizar vídeo. Esto se describe en este documento en Utilice un reproductor multimedia para ver una secuencia de vídeo (ver "Utilizar un reproductor multimedia para ver una secuencia de vídeo" en la página 425).

Se pueden utilizar diferentes puertos, por ejemplo, para evitar un conflicto de puertos. Si cambia los números de puerto, también debe actualizar la corriente RTSP para el cliente ONVIF URI.

RTSP sólo es compatible con el códec H.264. Las cámaras deben ser capaces de transmitir vídeo en el codec H.264.

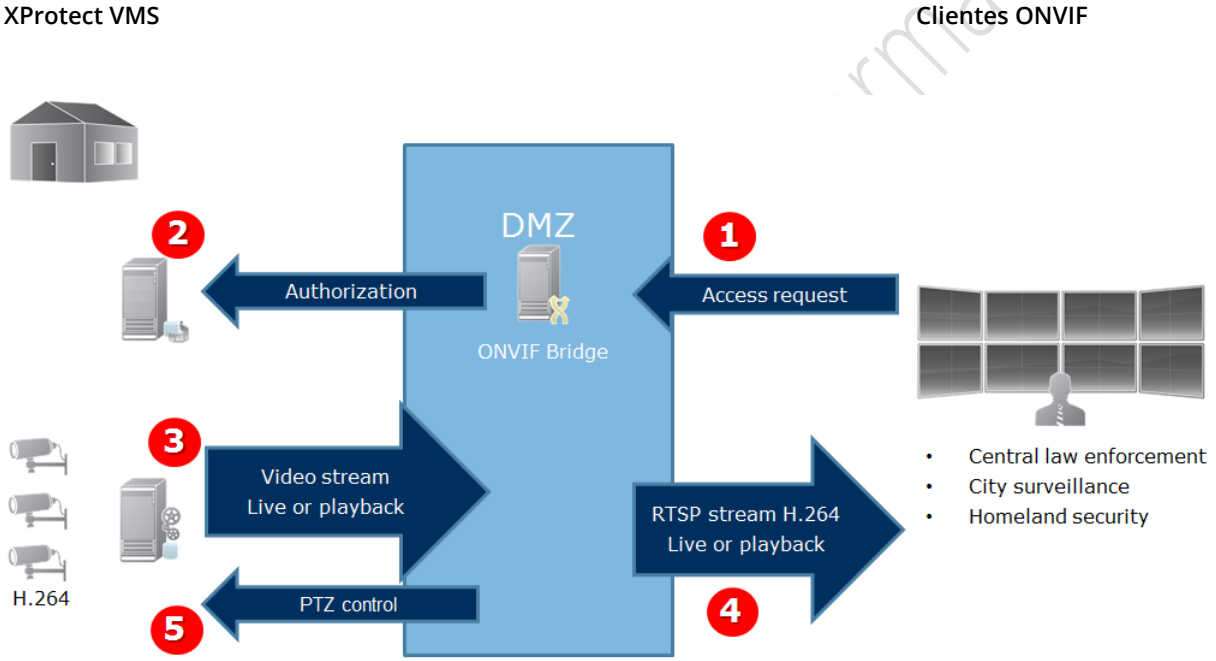
Milestone ONVIF Bridge

El Milestone ONVIF Bridge se compone de los siguientes componentes:

- Servidor Milestone ONVIF Bridge
- Milestone ONVIF Bridge 32 bits plug-in para Management Application
- Milestone ONVIF Bridge 64 bits plug-in para Management Client

La siguiente imagen muestra una vista de alto nivel de la interoperabilidad entre un cliente ONVIF, la Milestone ONVIF Bridge, y XProtect VMS.

Nota: Milestone recomienda instalar el servidor ONVIF Bridge en una zona desmilitarizada (DMZ).



1. Un cliente ONVIF se conecta al VMS XProtect a través del servidor ONVIF Bridge a través de Internet. Para ello, el cliente ONVIF necesita la dirección IP o el nombre de dominio (dominio / nombre de host) del servidor donde está instalado Milestone ONVIF Bridge y el número de puerto ONVIF.
2. El servidor ONVIF Bridge conecta con el servidor de administración para autorizar al usuario ONVIF cliente.
3. Después de la autorización, el servidor de grabación empieza a enviar H.264 flujos de vídeo de las cámaras al servidor ONVIF Bridge.

   Nota: Si una cámara es compatible con múltiples flujos, sólo se envía la corriente de defecto.
4. El servidor ONVIF Bridge envía el vídeo como flujos RTSP al cliente ONVIF.
5. Si está disponible, el usuario ONVIF cliente puede pan-tilt-zoom cámaras PTZ.

Configuración de controles de seguridad Milestone ONVIF Bridge

Milestone ONVIF Bridge hace cumplir la autorización del usuario de la ONVIF clientes. Esto controla la capacidad del cliente ONVIF acceder a las cámaras, y los tipos de operaciones de los ONVIF clientes pueden realizar. Por ejemplo, si los clientes pueden utilizar ONVIF giro, inclinación y zoom (PTZ) controles en las cámaras.

Milestone recomienda crear y añadir una cuenta de usuario dedicada para la Milestone ONVIF Bridge, y para cada cliente ONVIF, de la siguiente manera:

1. Cree un usuario básico en el Management Client, o un usuario de Windows.
2. En el Management Client, asigne al usuario una función que pueda acceder a las cámaras y especifique los permisos para el grupo de seguridad ONVIF Bridge en la ficha Seguridad general de la función.
3. Asigne al usuario Milestone ONVIF Bridge durante la instalación y en Management Client para cada cliente ONVIF posteriormente.

Milestone ONVIF Bridge permite sólo los clientes ONVIF a solicitar y recibir flujos de vídeo de las cámaras. ONVIF clientes no pueden establecer la configuración en el sistema VMS XProtect o la Milestone ONVIF Bridge.

Como medida de seguridad, Milestone recomienda instalar el servidor ONVIF Bridge en una zona desmilitarizada (DMZ). Si instala el puente en una DMZ, también debe configurar el reenvío de puertos para las direcciones IP internas y externas.

Instalación de Milestone ONVIF Bridge

Cuando instala Milestone ONVIF Bridge, instala un servidor y un complemento para el Management Client, que son los componentes de administración central para los productos XProtect VMS y XProtect Professional VMS, respectivamente. Por ejemplo, utiliza estos componentes para administrar cámaras, configurar los usuarios, conceder permisos, y así sucesivamente.

Puede instalar y añadir uno o más Milestone ONVIF Bridges a su sistema. Sin embargo, esto aumenta la carga en la red, y puede afectar al rendimiento. Por lo general, sólo una Milestone ONVIF Bridge se añade a un sistema ya varios ONVIF clientes pueden conectarse a través de un puente.

Licencias ONVIF

Milestone ONVIF Bridge no requiere licencias adicionales. Puede descargar e instalar el software de forma gratuita desde el sitio web Milestone Systems (https://www.milestonesys.com/support/resources/download-software/).

Requisitos del sistema

El equipo en el que desea instalar el componente Milestone ONVIF Bridge servidor debe tener acceso a Internet, y el siguiente software instalado:

- Microsoft® .NET Framework 3.5.
- Microsoft® . NET Framework 4.7 o superior.
- Visual C++ Redistributable Package de Visual Studio 2013 (x64).

Importante: Las cámaras deben apoyar H.264 el streaming a través de Internet.

¿Lo que está instalado?

Durante la instalación, se instalan los siguientes componentes:

- Milestone ONVIF Bridge servidor, incluyendo la Milestone ONVIF Bridge servicio, el servicio de Milestone RTSP Bridge, y el director Milestone ONVIF Bridge.
- Plug-in Milestone ONVIF Bridge. El complemento está disponible en el nodo Servidores en Management Client. Esto ocurre automáticamente cuando se utiliza método de instalación **típico**. Si utiliza un método de instalación **personalizado**, lo instala en una fase posterior de la instalación.

La instalación también hace lo siguiente:

- Registros e inicia el servicio Milestone ONVIF Bridge y el servicio Milestone RTSP Puente
- Inicia el Milestone ONVIF Bridge Manager, que está disponible en el área de notificación de Windows en el servidor donde está instalado el servidor ONVIF Bridge

Nota: Las acciones en el Administrador ONVIF Bridge se aplican tanto al servicio Milestone ONVIF Bridge y el servicio de Milestone RTSP Bridge. Por ejemplo, cuando se inicia o detiene el servicio ONVIF Bridge, el servicio de Milestone RTSP Bridge también se inicia o se detiene.

Antes de instalar

Antes de comenzar la instalación, obtener la siguiente información:

- El nombre de dominio y la contraseña de la cuenta de usuario dedicada que se creó para el Milestone ONVIF Bridge. Para obtener más información, consulte Configuración de controles de seguridad Milestone ONVIF Bridge (en la página 416).
- La dirección URL o IP y el número de puerto del servidor de administración.

Necesitará esta información durante la instalación.

Instalar el Milestone ONVIF Bridge

Descargar el archivo de instalación:

1. En el equipo en el que desea instalar Milestone ONVIF Bridge, vaya al sitio web (https://www.milestonesys.com/support/resources/download-software/) Milestone y localizar el producto Milestone ONVIF Bridge.
2. Haga clic en el archivo de instalación Milestone ONVIF Bridge.
3. Ejecute el instalador y siga las instrucciones.

Ejecutar el programa de instalación:

1. Seleccione el idioma que desea utilizar y, a continuación, haga clic en **Continuar**.
2. Lea y acepte el acuerdo de licencia y haga clic en **Continuar**.
3. Seleccionar el tipo de instalación, como sigue:

Para instalar el servidor ONVIF Bridge y plug-in en un equipo, y aplicar los ajustes predeterminados, haga clic Típico.

1. Compruebe que la URL del servidor, el nombre de usuario y la contraseña son correctos y haga clic en **Continuar**.

2. Seleccione la ubicación del archivo y el idioma del producto y haga clic en **Instalar**.

   Cuando la instalación se haya completado, una lista de componentes de pantallas instaladas correctamente. Haga clic en **Cerrar**.

Para instalar el servidor ONVIF Bridge y los complementos en equipos separados, haga clic en **Personalizado**. Utilice este método si tiene un sistema distribuido.

1. Para instalar el servidor, seleccione la casilla de verificación **Milestone ONVIF Bridge Server** y, a continuación, haga clic en **Continuar**.

2. Establezca una conexión con el servidor de administración especificando lo siguiente:

   - La dirección URL o IP y el número de puerto del servidor de administración. El puerto predeterminado es 80. Si omite el número de puerto, el sistema utilizará el puerto 80.
   - Mantenga el **Inicie sesión como** campo establecido en **Cuenta de usuario**.
   - El nombre de usuario y contraseña de dominio del usuario de Windows o de usuario básica que utilizará el servicio.
   - Haga clic en **Continuar**.

3. Seleccione la ubicación del archivo y el idioma del producto y haga clic en **Instalar**.

   Cuando la instalación se haya completado, una lista de componentes de pantallas instaladas correctamente.

4. Haga clic en **Cierre** y, a continuación, instale el complemento ONVIF Bridge en el equipo donde está instalado Management Client. Para instalar el complemento, vuelva a ejecutar el instalador en ese equipo, seleccione **Personalizado** y seleccione los respectivos complementos.

Los siguientes componentes ya están instalados:

- Servidor Milestone ONVIF Bridge
- Milestone ONVIF Bridge plug-in visible en Management Client en el nodo **Servidores**
- Milestone ONVIF Bridge Administrador que se está ejecutando y accesible desde el área de notificación del servidor con el servidor ONVIF Bridge instalado
- Milestone ONVIF Bridge servicio registrado como un servicio

Usted está listo para configuración inicial (ver "Configuración de la Milestone ONVIF Bridge" en la página 418).

Configuración de la Milestone ONVIF Bridge

Después de instalar el Milestone ONVIF Bridge, el servicio ONVIF Bridge se está ejecutando y el icono de la bandeja ONVIF Bridge Manager se vuelve verde. Los próximos pasos son:

- Añadir el complemento ONVIF Bridge al directorio Management Client
- Permita que los clientes de ONVIF accedan a su sistema XProtect

Agregue Milestone ONVIF Bridge al Management Client

1. Abra el Management Client.

2. Expandir **Servidores**, haga clic **ONVIF Bridge**, y seleccione **Añadir nuevo**.
3. Ingrese un nombre para Milestone ONVIF Bridge, y luego haga clic en **OK**.

Configurar opciones de usuario para un cliente ONVIF

Antes de poder completar estos pasos, debe haber creado un usuario básico en Management Client o un usuario de Windows para el cliente ONVIF. El usuario debe ser asignado a un cometido que tiene permiso para ver las cámaras y acceder a la Milestone ONVIF Bridge. Para obtener más información, consulte Configuración de controles de seguridad Milestone ONVIF Bridge (en la página 416). Para obtener información acerca de cómo configurar un usuario básico en Management Client, consulte la Ayuda para esos programas.

Para proporcionar un acceso de cliente ONVIF a su VMS XProtect, siga estos pasos:

1. Abra el Management Client.
2. Expandir **Servidores**, seleccione **ONVIF Bridge**, a continuación, seleccione el puente que acaba de añadir.
3. En la pestaña **Configuración de usuario**, introduzca el nombre de usuario de dominio (dominio / usuario) y la contraseña del usuario dedicada creado para el cliente ONVIF.
4. Haga clic en el botón **Añadir usuario**.

El nombre del usuario ONVIF cliente aparece en la lista de los **ONVIF credenciales de usuario**.

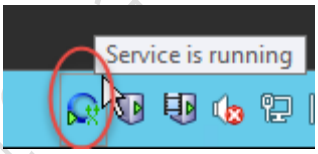
La gestión de Milestone ONVIF Bridge

Después de configurar el Milestone ONVIF Bridge, puede supervisar el servicio y cambiar la configuración de varias maneras.

Comprobar el estado del servicio ONVIF Bridge

Para ver el estado del servicio ONVIF Bridge, siga estos pasos.

1. En el equipo donde está instalado el servidor ONVIF Bridge, busque en el área de notificación. El icono de la bandeja de ONVIF Bridge Manager indica el estado del servicio ONVIF Bridge. Si el servicio se está ejecutando, el icono es de color verde.

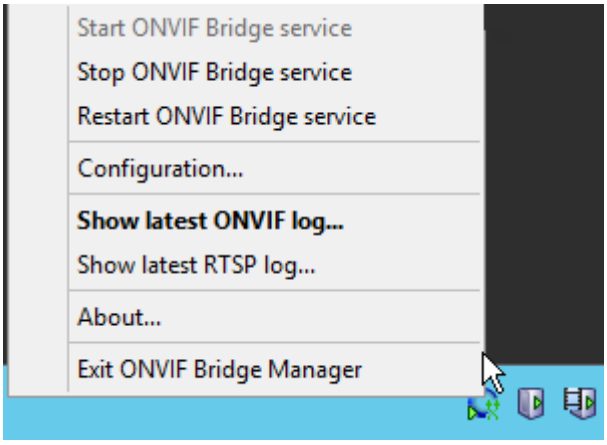


2. Si no se está ejecutando, el icono es de color amarillo o rojo. Haga clic en el icono y seleccione el **servicio Start ONVIF Bridge**.

Ver los registros

El ONVIF Bridge Manager guarda la información de registro del servidor ONVIF Bridge y los flujos RTSP.

1. En el área de notificación en la computadora donde está instalado el servidor ONVIF Bridge, haga clic con el botón derecho en el ícono de la bandeja de ONVIF Bridge Manager.



2. Seleccione **Ultimas registro ONVIF** o **Mostrar registro más reciente RTSP**.

Cambiar el nivel de información de los registros

El ONVIF Bridge Manager guarda la información de registro del servidor ONVIF Bridge y los flujos RTSP.

Para cambiar el nivel de información, siga estos pasos:

1. Haga clic con el botón derecho en el icono de la bandeja de ONVIF Bridge Manager y luego detenga el servicio ONVIF Bridge.
2. Haga clic con el botón derecho en el ícono de la bandeja de ONVIF Bridge Manager nuevamente y seleccione **Configuración**.
3. En los campos **Nivel de registro para ONVIF** y **Nivel de registro para RTSP**, especifique el tipo de información y la cantidad de información que desea guardar en los registros ONVIF y RTSP. El valor por defecto es **Información**.

   Nota: De arriba a abajo en la lista, las opciones están ordenados de menor nivel a mayor nivel. Cada nivel incluye el nivel por encima de ella en la lista. Por ejemplo, el nivel de **Advertencia** incluye el nivel de **Error**. Milestone recomienda que utilice sólo niveles **Error**, **Advertencia** y **Información**. Los niveles **Rastro** y **Mensaje** capturar más información y utilizan más espacio en disco, lo que puede disminuir el rendimiento.

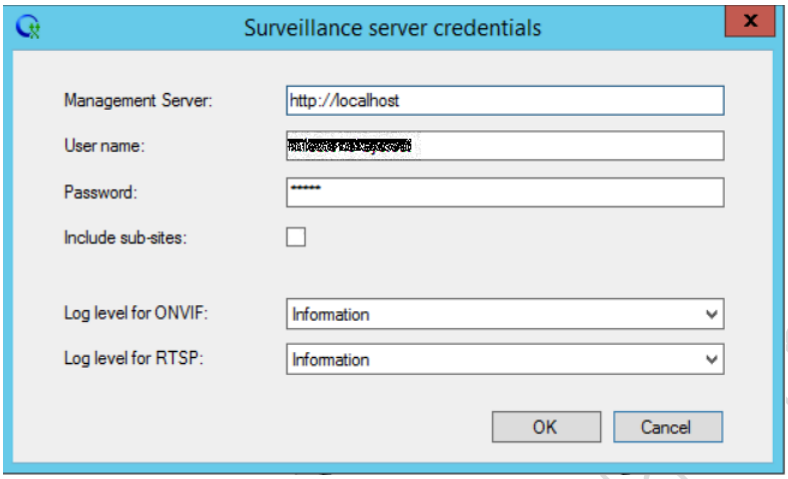
4. **Haga clic en OK (aceptar)**.
5. Haga clic con el botón derecho en el icono de la bandeja de ONVIF Bridge Manager y luego inicie el servicio ONVIF Bridge.

Cambiar la configuración de configuración para el Milestone ONVIF Bridge

Si cambia la dirección IP o nombre de host del servidor de vigilancia, o si ha cambiado las cuentas de usuarios que tienen acceso al servicio de servidor de vigilancia, debe actualizar esta información para Milestone ONVIF Bridge.

Para cambiar la dirección de VMS o credenciales de acceso, siga estos pasos:

1. En la computadora donde está instalado el servidor Milestone ONVIF Bridge, haga clic con el botón derecho en el icono de la bandeja de ONVIF Bridge Manager y luego detenga el servicio ONVIF Bridge.
2. Haga clic con el botón derecho en el ícono de la bandeja de ONVIF Bridge Manager nuevamente y seleccione **Configuración**.



3. Especifique la nueva información y, a continuación, haga clic en **Aceptar**.

Nota: Debe utilizar el nombre de dominio completo o la dirección IP del servidor donde está instalado el servidor de gestión.

4. Haga clic con el botón derecho en el icono de la bandeja de ONVIF Bridge Manager y luego inicie el servicio ONVIF Bridge.

El servicio de ONVIF Bridge está en funcionamiento y el icono de la bandeja se vuelve verde.

Incluir sitios secundarios

Por defecto, el Milestone ONVIF Bridge está configurado para excluir sub-sitios. Esto significa que los usuarios de ONVIF clientes no pueden acceder a vídeo de las cámaras que están instaladas en sitios secundarios.

Puede cambiar esto para incluir sitios secundarios. Sin embargo, Milestone recomienda que lo haga sólo para sistemas en los que los sitios secundarios no contienen un gran número de cámaras. El Milestone ONVIF Bridge agrupa y muestra todas las cámaras, incluidas las de sitios secundarios, en una lista. Por ejemplo, si el sistema y sitios secundarios tienen más 50 cámaras, la lista será difícil de usar.

Consejo: Si debe incluir sitios secundarios, considere la instalación de la Milestone ONVIF Bridge en cada servidor de gestión. Tendrá más de una lista de cámaras, sin embargo, las cámaras serán más fáciles de identificar y navegar.

Para incluir sitios secundarios:

1. Haga clic con el botón derecho en el icono de la bandeja de ONVIF Bridge Manager y luego detenga el servicio ONVIF Bridge.
2. Haga clic con el botón derecho en el ícono de la bandeja del ONVIF Bridge Manage nuevamente y haga clic en **Configuración**.
3. Seleccione la casilla **Incluir sitios secundarios** y, a continuación, haga clic en **Aceptar**.

4. Haga clic con el botón derecho en el icono de la bandeja de ONVIF Bridge Manager y luego inicie el servicio ONVIF Bridge.

Consejos y trucos

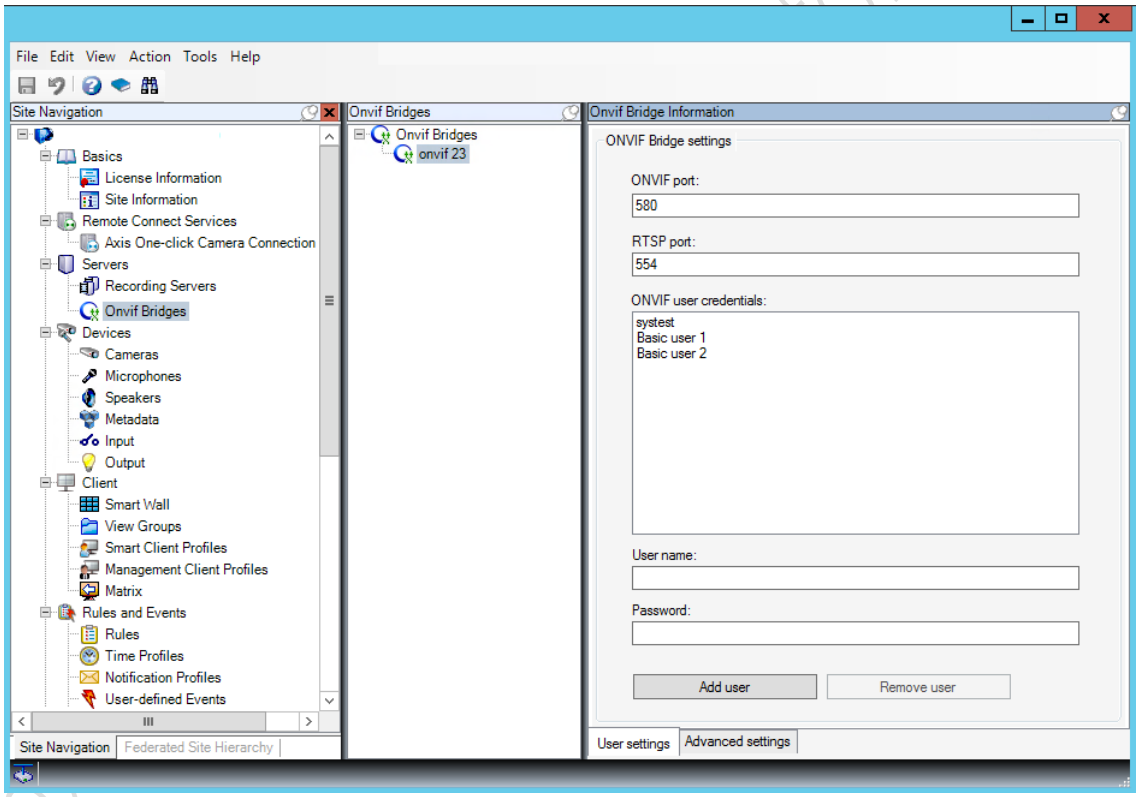
La configuración creada por ONVIF Bridge Manager se almacena localmente en un archivo en ProgramData\Milestone\XProtect ONVIF Bridge. El nombre del archivo es serverconfiguration.xml. Si se elimina este archivo, debe actualizar la configuración en ONVIF Bridge Manager.

Para actualizar una configuración, siga los pasos descritos en Cambiar configuración para un Milestone ONVIF Bridge en este documento.

Propiedades Milestone ONVIF Bridge

Esta sección incluye información sobre los ajustes para administrar los usuarios y las conexiones y los ajustes de configuración para las cámaras.

Abra el Management Client y seleccione el nodo **ONVIF Bridge**.



Pestaña de configuración de usuario (propiedades)

En la siguiente tabla se describen los ajustes para el servidor ONVIF Bridge y clientes ONVIF.

Nombre	Descripción
Puerto ONVIF	El número de puerto del puerto ONVIF. ONVIF clientes utilizan este puerto para conectarse al servidor ONVIF Bridge. El número de puerto predeterminado es 580.

Nombre	Descripción
Puerto RTSP	El número de puerto del puerto RTSP. El servidor envía ONVIF Bridge RTSP flujos de vídeo a través de este puerto para ONVIF clientes. El número de puerto predeterminado es 554.
Credenciales de usuario ONVIF	Lista los usuarios del cliente ONVIF que tienen acceso al sistema XProtect VMS a través del servidor ONVIF Bridge.
Nombre de usuario	El nombre de usuario de dominio del usuario creado para un cliente ONVIF. Requisito: Debe configurar los usuarios de cliente ONVIF como usuarios en Management Client con acceso a cámaras y Milestone ONVIF Bridge.
Contraseña	La contraseña para el usuario ONVIF cliente.
Añadir usuario	Después de introducir un nombre de usuario y contraseña del dominio, haga clic en el botón **Añadir usuario** para añadir el usuario.
Eliminar usuario	Evitar que un cliente ONVIF acceda a la Milestone ONVIF Bridge. Eliminar un usuario seleccionado de la **ONVIF credenciales de usuario** lista.

Pestaña de configuración avanzada (propiedades)

La configuración avanzada para el ONVIF Bridge lista de los ajustes por defecto para todas las cámaras que el ONVIF Bridge proporciona a los clientes ONVIF cuando los clientes se conectan y flujos solicitud de vídeo.

Los ajustes no reflejan la configuración real de las cámaras, y no afectan a la secuencia de vídeo. El sistema utiliza la configuración para acelerar el intercambio de vídeo entre la ONVIF Bridge y el cliente ONVIF. El cliente ONVIF utilizará la configuración real de la corriente RTSP.

Puede cambiar la configuración predeterminada que ONVIF Bridge proporciona al cliente ONVIF, por ejemplo, si desea que los valores que reflejan la configuración real de las cámaras.

Nombre	Descripción
Número máximo de días de retención	El valor por defecto es 30.
Fotogramas por segundo	El valor por defecto es 5.
Ancho	El valor por defecto es 1920. Esto corresponde a una calidad HD.
Altura	El valor por defecto es 1080. Esto corresponde a una calidad HD.
Kbps de velocidad de bits	El valor por defecto es 512.
El tamaño de GOP	El valor por defecto es 5.
Codificador	Seleccione uno de los perfiles de códec H.264. El valor por defecto es H.264 perfil básico.
Utilizar las configuraciones de las cámaras	Activar esta opción para utilizar la configuración real de las cámaras en lugar de los valores medios predeterminados definidos anteriormente. **Nota:** Si se habilita esta configuración, el tiempo de respuesta entre el sistema XProtect y los clientes ONVIF aumenta.

Nombre	Descripción
Regresa las secuencias en el comando	Habilite esto para devolver información para secuencias en la respuesta de comando DESCRIBE.
Número máximo a devolver	Establezca el número máximo de secuencias que se enviarán al cliente. El valor predeterminado es 10.
Regresar desde el inicio o el final de la grabación	Seleccione desde dónde empezar a buscar las secuencias. Desde el principio o desde el final de la grabación.
Preferir tiempo absoluto sobre normalizado	Esta configuración define la respuesta de reproducción del servidor RTSP, en la que no se especifica el intervalo de tiempo del cliente para la reproducción. Seleccione esta opción si desea que su servidor RTSP utilice el tiempo real en contraposición a la reproducción escalada o normalizada. Sin embargo, si su aplicación cliente está configurada para utilizar intervalos de tiempo relativos o intervalos de tiempo real (en UTC), el servidor RTSP responde con los intervalos definidos en el cliente.

Usando clientes ONVIF para ver secuencias de vídeo

ONVIF clientes pueden ser muchas cosas diferentes, que van desde los sistemas de vigilancia avanzados personalizados a los jugadores básicos de medios de comunicación.

Esta sección proporciona ejemplos de cómo conectarse al Milestone ONVIF Bridge.

Utilice una Video Client red para ver una transmisión en vivo

En este ejemplo se describe cómo instalar ONVIF Device Manager y configurarlo para transmitir vídeo en directo desde una instalación XProtect.

El Administrador de dispositivos es un ONVIF, red de código abierto Video Client iDeviceDesign de que cumpla con las normas ONVIF. La herramienta se utiliza ampliamente para, ya que hace que sea fácil de descubrir y ver el vídeo de las cámaras ONVIF compatibles en una red. Tenga en cuenta, sin embargo, que utiliza ONVIF Administrador de dispositivos para transmitir sólo viven de vídeo. Además, no se puede capturar y guardar los datos de vídeo en la corriente.

Antes de empezar, obtenga la siguiente información de la persona que administra la instalación XProtect:

- Las credenciales de inicio de sesión para el usuario que se creó para la Milestone ONVIF Bridge

La dirección IP o el equipo nombre del equipo donde está instalado el Milestone ONVIF Bridge Para instalar el Administrador de dispositivos ONVIF, siga estos pasos:

1. Vaya al Sourceforge ONVIF sitio del Administrador de dispositivos (https://sourceforge.net/projects/onvifdm) y luego descargar y ejecutar el instalador. Puede instalar el Administrador de dispositivos ONVIF en cualquier ordenador.

2. Cuando se completa la instalación, un icono está disponible en el escritorio. Haga doble clic en el icono para iniciar el Administrador de dispositivos ONVIF.

3. Al iniciar el Administrador de dispositivos ONVIF, que detecta automáticamente los dispositivos compatibles con ONVIF en la red. Sin embargo, podría no descubrir la Milestone ONVIF Bridge.

    - Si es así, vaya al paso 6.

- Si no lo hace, añadir el puente manualmente. Continúe con el paso 4.

4. Para añadir un Milestone ONVIF Bridge, haga clic **Añadir**.
5. En el cuadro **Añadir dispositivo**, en el campo **URI**, indique el nombre o la dirección IP del equipo donde está instalado Milestone ONVIF Bridge y el número de puerto ONVIF. Por ejemplo, la cadena debe tener este aspecto: http://[IP address]:580/onvif/device_service
6. Después de añadir el puente, está disponible en la parte inferior de la lista **Dispositivo**. Seleccionarlo.
7. Introduzca las credenciales de inicio de sesión para el usuario básico que se creó para el cliente ONVIF superior de la lista. Para obtener el nombre de usuario, debe introducir el nombre de usuario de dominio.
8. Reinicie el servicio ONVIF Bridge para aplicar el cambio.

Utilizar un reproductor multimedia para ver una secuencia de vídeo

En este ejemplo se describe cómo utilizar el reproductor de medios VLC para recuperar y ver una alimentación de vídeo en directo o un vídeo grabado desde una cámara en una instalación XProtect.

VLC Media Player es un reproductor de código abierto libre de multimedia desde VideoLan que soporta varios protocolos de streaming, incluyendo RTSP. Por ejemplo, el uso de VLC media player es útil cuando se desea una manera muy rápida para conectarse a una cámara, o simplemente para probar la conexión a una cámara.

Cuando se conecta a una cámara para ver el vídeo grabado, la Milestone ONVIF Bridge flujos de las secuencias de vídeo, comenzando con la primera secuencia.

Antes de empezar, obtenga la siguiente información de la persona que administra la instalación XProtect:

- Las credenciales de inicio de sesión para la cuenta de usuario que se asigna a la Milestone ONVIF Bridge.
- La dirección IP o el equipo nombre del equipo donde está instalado el Milestone ONVIF Bridge
- El GUID del dispositivo que desea transmitir vídeo desde.

Consejo: El GUID de la cámara está disponible en Management Client. Para encontrar el GUID, seleccione el servidor de grabación donde se ha añadido la cámara, y luego seleccionar la cámara. Haga clic en la pestaña **Info**, mantenga presionado la tecla CTRL del teclado y haga clic en vista previa de vídeo de la cámara.

Esta descripción se basa en VLC 2.2.4 para Windows.

Para instalar el reproductor multimedia VLC y conectarlo a un sistema XProtect, siga estos pasos:

1. Ir a http://www.videolan.org/vlc/index.html, y luego descargar el instalador para el reproductor multimedia VLC.
2. Ejecutar el programa de instalación y siga las instrucciones para cada paso.
3. En la barra de herramientas, haga clic **Medios** y seleccione **Abrir Network Stream**.
4. En el cuadro de diálogo **Abrir medio**, ingrese la siguiente cadena RSTP. Reemplace las variables entre corchetes [Dirección IP de ONVIF Bridge] y [Camera GUID] con la información correcta:
   - Para ver una transmisión de video en vivo, ingrese rtsp://[ONVIF Bridge IP Address]:554/live/[Camera GUID]
   - Para ver video grabado, ingrese rtsp://[ONVIF Bridge IP Address]:554/vod/[Camera GUID]

5. Haga clic en **Reproducir**, a continuación, introduzca el nombre de usuario y la contraseña de la cuenta de usuario que se agregó a la Milestone ONVIF Bridge.

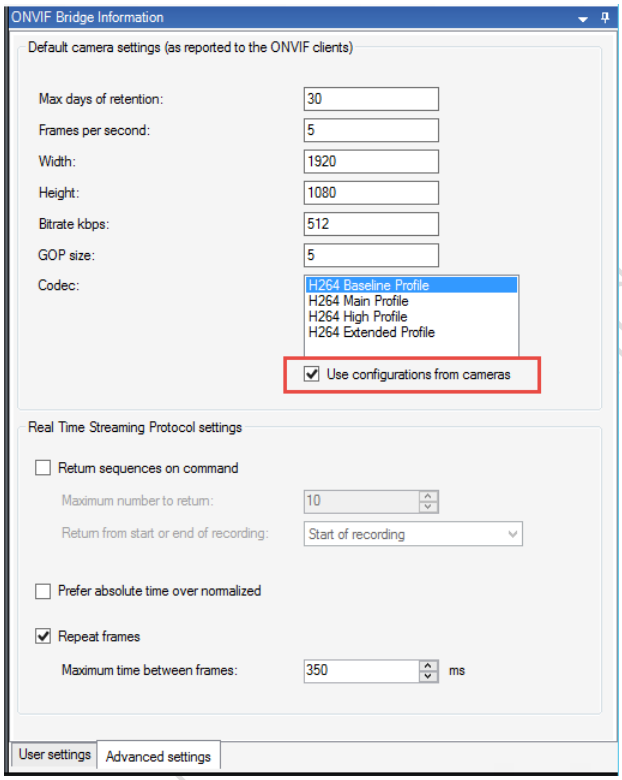
Administrar reproducción de vídeo

Los controles de reproducción cumplen con los estándares RTSP y la especificación de transmisión ONVIF (http://www.onvif.org/specs/stream/ONVIF-Streaming-Spec-v210.pdf).

Registro de resumen

Puede obtener una descripción general de todos los videos grabados disponibles en el dispositivo utilizando el comando `GetRecordingSummary`. Esto no es obligatorio, pero proporciona información útil antes de realizar una búsqueda.

Puede utilizar `GetRecordingSummary` y / o `GetMediaAttributes` para obtener la marca de tiempo de la primera y la última grabación, pero primero debe habilitar **Usar configuraciones de cámaras** en la ficha **Configuración avanzada** en el plug-in Milestone ONVIF Bridge en el XProtect Management Client.



Cree un proxy para el servicio `RecordingSearch` utilizando el punto final del servicio devuelto por `GetServices`. Cree objetos de solicitud y respuesta, luego llame al `GetRecordingSummary`.

```
SearchBindingProxy searchProxy( &soapSearch );
std::string searchEndpoint = "http://" + host +
"/onvif/recording_search_service";
_tse__GetRecordingSummary tse__GetRecordingSummary;
_tse__GetRecordingSummaryResponse tse__GetRecordingSummaryResponse;
result = searchProxy.GetRecordingSummary( searchEndpoint.c_str(), NULL,
    &tse__GetRecordingSummary, &tse__GetRecordingSummaryResponse );
```

Buscar grabaciones

El método de servicio de búsqueda `FindRecordings` inicia una búsqueda asincrónica en la cámara. `FindRecordings` devuelve un token que hace referencia a los resultados de búsqueda. Aunque solo hay una grabación disponible, una búsqueda es la forma correcta de obtener una referencia para esa grabación.

Enviar una solicitud `FindRecordings` con los siguientes parámetros obligatorios:

- `SearchScope` > `IncludedSources` > `Token` - debe proporcionar el token de GUID de la cámara
- `SearchScope` > `RecordingInformationFilter` - cadena con los siguientes parámetros:
  - `marca de tiempo` (en formato UTC)
  - `maxTimeBefore` (el tiempo antes de la marca de tiempo solicitada, en milisegundos)
  - `maxCountBefore` (la cantidad máxima de pistas antes de la marca de tiempo solicitada)
  - `maxTimeAfter` (el tiempo después de la marca de tiempo solicitada, en milisegundos)
  - `maxCountAfter` (la cantidad máxima de pistas después del sello de tiempo solicitado)

Por ejemplo:

```
boolean(//Track[TrackType = “Video”]),2016-12-
06T08:07:43Z,99999999,20,99999999,20
```

Obtendrá una respuesta con un `SearchToken`, que es único para los criterios de búsqueda.

Pase `SearchToken` a `GetRecordingSearchResults` y obtendrá una lista con todas las pistas correspondientes a los criterios de búsqueda.

Inicio de la reproducción

Cuando se visualiza la reproducción de vídeo, la velocidad predeterminada es 1 (reproducción normal en la dirección hacia adelante).

La reproducción se inicia mediante el método RTSP PLAY. Se puede especificar un rango. Si no se especifica ningún rango, el flujo se reproduce desde el principio y se reproduce hasta el final, o, si el flujo está en pausa, se reanuda en el punto en que se hizo una pausa. En este ejemplo, "Rango: npt = 3-20" indica al servidor RTSP que inicie la reproducción desde el 3º al segundo hasta el 20º segundo.

Por ejemplo:

```
PLAY rtsp://basic:basic@bgws-pvv-04:554/vod/943ffaad-42be-4584-bc2c-
c8238ed96373 RTSP/1.0
CSeq: 123
Sesión: 12345678
Requerir: onvif-replay
Rango: npt = 3-20
Control de tasas: no
```

Reproducción inversa

Los dispositivos ONVIF PUEDEN soportar la reproducción inversa. La reproducción inversa se indica utilizando el campo de cabecera Escala con un valor negativo. Por ejemplo, para jugar al revés sin pérdida de datos, se utilizaría un valor de -1.0.

El Milestone ONVIF Bridge admite valores [-32: 32].

```
PLAY rtsp://basic:basic@bgws-pvv-04:554/vod/943ffaad-42be-4584-bc2c-
c8238ed96373 RTSP/1.0
CSeq: 123
Sesión: 12345678
Requerir: onvif-replay
Distancia: reloj = 20090615T114900.440Z
Control de tasas: no
Escala: -1.0
```

Cambiar velocidad

La velocidad es controlada por el encabezado RTSP Rate-Control. Si "Rate-Control = yes", el servidor tiene el control de la velocidad de reproducción. El flujo se entrega en tiempo real utilizando mecanismos de temporización RTP estándar. Si "Rate-Control = no", el cliente tiene el control de la velocidad de reproducción. La repetición controlada por frecuencia normalmente solo será utilizada por clientes que no sean de ONVIF porque no especificarán "Control de frecuencia = no".

Para controlar la velocidad de reproducción en un cliente, use los controladores provistos. Por ejemplo, con el reproductor multimedia VLC, seleccione **Reproducción** > **Velocidad** > **Más rápido** o **Más lento**. Esto aumenta o disminuye la velocidad en 0.5.

Más rápido Fino y **Más lento Fino** cambiar la velocidad en 0.25.

Administrar la reproducción del reproductor de medios VLC con las entradas de la línea de comandos

Puede administrar la reproducción de vídeo en el reproductor de medios VLC utilizando líneas de comando. Consulte la ayuda de la línea de comandos VLC (https://wiki.videolan.org/VLC_command-line_help/) para obtener más detalles.

Tales comandos le permiten, por ejemplo, invertir la reproducción y cambiar la hora de inicio de la reproducción.

Un ejemplo de una línea de comandos típica:

```
>vlc.exe --rate=-1.0 --start-time=3600 "rtsp://basic:basic@bgws-pvv-
04:554/vod/943ffaad-42be-4584-bc2c-c8238ed96373"
```

Dónde:

- la tasa es el parámetro de escala y velocidad
- La hora de inicio es de segundos después del inicio de la base de datos

Los siguientes son los controles de reproducción del reproductor multimedia VLC:

Input-repeat =	<integer [-2147483648 .. 2147483647]> Repeticiones de entrada Número de veces que se repetirá la misma entrada
start-time=	<float> Hora de inicio El flujo comenzará en esta posición (en segundos)

stop-time=	<float> Hora de la parada El flujo se detendrá en esta posición (en segundos)
run-time=	<float> Tiempo de ejecución El flujo ejecutará esta duración (en segundos)
input-fast-seek No-input-fast-seek	Búsqueda rápida (predeterminada deshabilitada) Favorecer la velocidad sobre la precisión mientras busca
rate=	<float> Velocidad de reproducción Esto define la velocidad de reproducción (la velocidad nominal es 1,0)
Input-list =	<string> Lista de entradas Puede dar una lista separada por comas de entradas que se concatenarán juntas después de la normal
Input-slave =	<string> Esclavo de entrada (experimental) Esto le permite reproducir varias entradas al mismo tiempo. Esta característica es experimental, no todos los formatos son compatibles. Utilice una lista de entradas separadas con un '#'
bookmarks=	<string> Lista de marcadores para un flujo Puede proporcionar manualmente una lista de marcadores para un flujo en el formato "{name=bookmark-name,time=optional-time-offset,bytes=optional-byte-off set},{...}"

XProtect DLNA Server

En esta sección, puede leer acerca del soporte de DLNA (Digital Living Network Alliance) en sistemas XProtect. Encontrará instrucciones sobre cómo instalarlo y configurarlo.

XProtect DLNA Server (explicado)

DLNA (Digital Living Network Alliance) es un estándar para conectar dispositivos multimedia. Los fabricantes electrónicos obtienen sus productos certificados por DLNA para asegurar la interoperabilidad entre diferentes proveedores y dispositivos y así permitirles distribuir contenido multimedia como audio, video y fotos.

Las pantallas públicas y los televisores a menudo están certificados por DLNA y conectados a una red. Pueden escanear la red en busca de contenido multimedia, conectarse al dispositivo y solicitar un flujo multimedia a su reproductor multimedia incorporado. XProtect DLNA Server puede ser descubierto por ciertos dispositivos certificados por DLNA y entregar flujos de vídeo en vivo desde cámaras seleccionadas a dispositivos certificados DLNA con un reproductor multimedia.

Nota: Los dispositivos DLNA tienen un retraso de video en vivo de 1-10 segundos. Esto se debe a diferentes tamaños de búfer en los dispositivos.

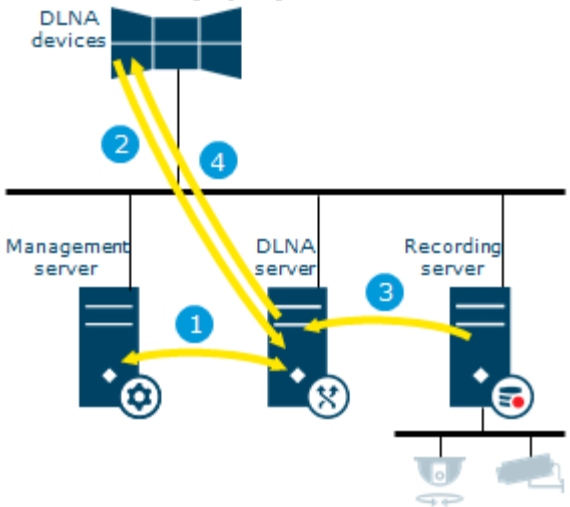
XProtect DLNA Server debe estar conectado a la misma red que el sistema XProtect y el dispositivo DLNA debe estar conectado a la misma red que XProtect DLNA Server.

XProtect DLNA Server flujo del sistema

El XProtect DLNA Server se compone de los siguientes componentes:

- XProtect DLNA Server
- XProtect DLNA Server 64-bit admin plug-in para el Management Client

La ilustración siguiente muestra una vista de alto nivel de la interoperabilidad entre un dispositivo DLNA y XProtect DLNA Server en el sistema XProtect.



1. Durante el arranque del servicio XProtect DLNA Server, el XProtect DLNA Server se conecta al servidor de administración para autorizarse a sí mismo con las credenciales proporcionadas. Después de la autorización, el XProtect DLNA Server se inicia y está listo para enviar flujos de vídeo H.264 de las cámaras a los dispositivos DLNA.

2. Un dispositivo DLNA se conecta al sistema XProtect a través del XProtect DLNA Server y solicita un flujo de video de cámara en directo. Para ello, el dispositivo DLNA necesita la dirección IP o el nombre de dominio (dominio / nombre de host) del servidor donde se instala XProtect DLNA Server y el número de puerto DLNA. Esto se hace automáticamente por el protocolo UPnP.
3. XProtect DLNA Server recupera la secuencia de vídeo de la cámara solicitada del servidor de grabación.
4. XProtect DLNA Server envía la secuencia de vídeo en directo de la cámara solicitada a través de HTTP streaming al dispositivo DLNA.

Nota: Sólo se admite el flujo de cámaras codificadas en H.264. Si una cámara es compatible con múltiples flujos, sólo se envía la corriente de defecto.

Antes de comenzar la instalación

Cuando instala XProtect DLNA Server, instala un servidor y un complemento para el Management Client. Estos componentes le permiten agregar canales DLNA y proporcionar vídeo a dispositivos DLNA.

Puede instalar y agregar varios servidores DLNA a su sistema XProtect. Tenga en cuenta que múltiples dispositivos DLNA pueden conectarse a cada servidor DLNA, por lo que aumenta la carga en la red y puede afectar el rendimiento. Para reducir el uso general de los recursos de red en la computadora que ejecuta el servidor de gestión, instale XProtect DLNA Server en una computadora separada.

Nota: La instalación requiere un reinicio del servicio Event Server y Management Client

Milestone recomienda que siga la preparación que se describe en las siguientes secciones, antes de comenzar la instalación real.

Licencia

XProtect DLNA Server no requiere licencias adicionales. Puede descargar e instalar el software de forma gratuita desde la página web de instalación administrativa del servidor de gestión.

Requisitos del sistema

La computadora donde desea instalar el componente XProtect DLNA Server tiene estos requisitos:

- Conectado a la misma red que el sistema XProtect
- Acceso al servidor de gestión
- Microsoft® .NET Framework 4.5.1 o superior instalado

Para obtener información acerca de los requisitos **mínimos** del sistema para los distintos componentes de su sistema, vaya al sitio web (https://www.milestonesys.com/support/resources/system-requirements) Milestone.

Qué está instalado

Durante la instalación, se instalan los siguientes componentes:

- XProtect DLNA Server Plug-in de administración
- XProtect DLNA Server que incluye:
  - XProtect DLNA Server Administrador que se está ejecutando y accesible desde el área de notificación en el servidor con XProtect DLNA Server instalado
  - Servicio XProtect DLNA Server

La instalación también hace lo siguiente:

- Registra e inicia el servicio XProtect DLNA Server
- Inicia el Administrador XProtect DLNA Server, que está disponible en el área de notificación de Windows en el servidor donde está instalado XProtect DLNA Server

Nota: El complemento está disponible en el nodo **Servidores** en el Management Client. Esto ocurre automáticamente cuando se utiliza método de instalación **típico**. Si utiliza un **Custom** método de instalación, puede instalarlo en una fase posterior de la instalación.

Ajustes de cámara

Verifique la configuración de cámara recomendada en el Management Client:

- Cuadros por segundo: **25** (o más).
- Máximo de marcos entre fotogramas clave: **25** (el mismo valor que los fotogramas por segundo).
- Resolución: **1920x1080**.
- Modo de control de velocidad de bits: **Velocidad de bits constante**.

Installer XProtect DLNA Server

Para acceder a la página web de instalación:

1. Inicie sesión en la computadora donde desea instalar el XProtect DLNA Server y abra un navegador de Internet.
2. Introduzca la siguiente URL en el navegador: http://[dirección del servidor de gestión]/installation/admin

   [management server address] es la dirección IP o nombre de host del servidor de gestión.
3. Seleccione **Todos los idiomas** debajo del **instalador del servidor DLNA** .
4. Haga clic en **Guardar** para guardar el instalador en un lugar apropiado y ejecutarlo desde aquí o haga clic en **Ejecutar** para ejecutarlo directamente desde la página web.

Ejecutar el programa de instalación:

1. Acepte todas las advertencias y seleccione el idioma que desea usar. Haga clic en **Continuar**.
2. Lea y acepte el contrato de licencia. Haga clic en **Continuar**.
3. Seleccionar el tipo de instalación, como sigue:
   - En un sistema de computadora individual, seleccione **Típica** (ver "**Instalación típica**" en la página 433).
   - En un sistema distribuido, seleccione **Personalizado** (ver "**Instalación personalizada**" en la página 433).

Instalación típica

1. Para instalar todos los componentes XProtect DLNA Server en un equipo y aplicar la configuración predeterminada, haga clic en **Típico**.
   - La dirección URL o IP y el número de puerto del servidor de gestión. El puerto predeterminado es 80. Si omite el número de puerto, el sistema utilizará el puerto 80.
   - Compruebe que el inicio de sesión como NETWORK SERVICE (servicio de red) o una cuenta de usuario especificada con **nombre de usuario** y **contraseña** es correcta.
   - Haga clic en **Continuar**.
2. Seleccione la ubicación del archivo y el idioma del producto y haga clic en **Instalar**.

   Cuando se completa la instalación, aparece una lista de componentes instalados correctamente. Haga clic en **Cerrar**.
3. Reinicie el servicio Event Server y luego el Management Client.

A continuación, Configurando XProtect DLNA Server (ver "Configurar XProtect DLNA Server" en la página 434).

Instalación personalizada

1. Para instalar componentes XProtect DLNA Server en equipos separados, haga clic en **Personalizado**.
2. Para instalar el servidor, seleccione la casilla de verificación **XProtect DLNA Server** y, a continuación, haga clic en **Continuar**.
3. Especifique los puertos para la comunicación con el XProtect DLNA Server:
   - Los números de puerto predeterminados son: DLNA video **9200**, dispositivo DLNA **9100** y configuración **9300**.
   - Haga clic en **Continuar**.
4. Establezca una conexión con el servidor de gestión especificando lo siguiente:
   - La dirección URL o IP y el número de puerto del servidor de gestión. El puerto predeterminado es 80. Si omite el número de puerto, el sistema utilizará el puerto 80.
   - Compruebe que el inicio de sesión como NETWORK SERVICE (servicio de red) o una cuenta de usuario especificada con **nombre de usuario** y **contraseña** es correcta.
   - Haga clic en **Continuar**.
5. Seleccione la ubicación del archivo y el idioma del producto y haga clic en **Instalar**.

   Cuando se completa la instalación, aparece una lista de componentes instalados correctamente.
6. Haga clic en **Cierre**e instale el complemento XProtect DLNA Server en el equipo donde está instalado el Management Client. Para instalar el complemento, vuelva a ejecutar el instalador en ese equipo, seleccione **Personalizado** y seleccione el complemento.
7. Reinicie el servicio Event Server y luego el Management Client.

A continuación, Configurando XProtect DLNA Server (ver "Configurar XProtect DLNA Server" en la página 434).

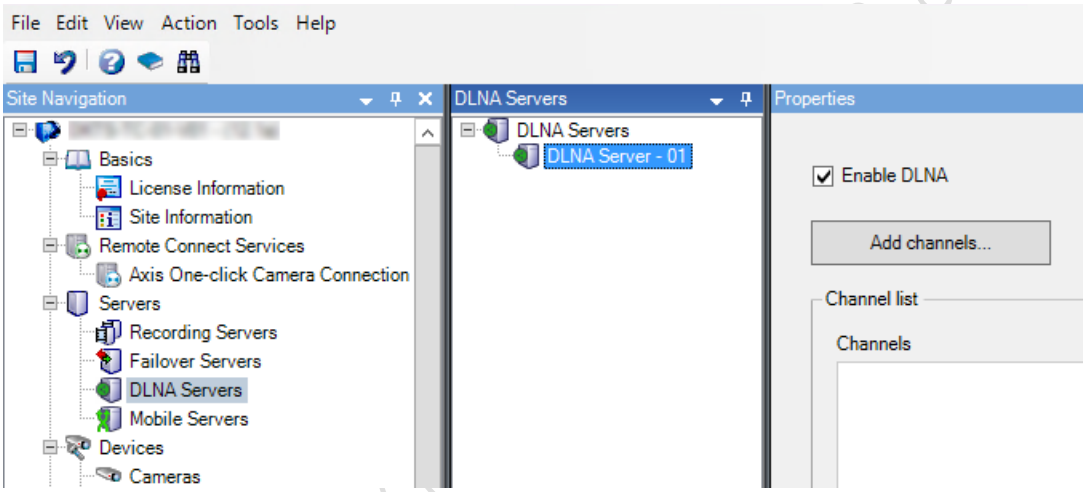
Configurar XProtect DLNA Server

Después de instalar XProtect DLNA Server, se está ejecutando el servicio XProtect DLNA Server y el icono del DLNA Server Manager en la bandeja del sistema se vuelve verde. El siguiente paso es hacer que las cámaras estén disponibles para XProtect DLNA Server.

Configurar la configuración de un servidor DLNA

Para proporcionar un acceso de dispositivo DLNA a su XProtect VMS, siga estos pasos:

1. Abra el Management Client.
2. Expanda **Servidores**, seleccione **Servidores DLNA**y, a continuación, seleccione el servidor DLNA que acaba de agregar.



3. Para cambiar el nombre del servidor, haga clic con el botón derecho en el servidor DLNA y seleccione **Rename**. El nombre que ingresa es el nombre que descubren los dispositivos DLNA durante el escaneo del contenido disponible de los medios.
4. En la ficha **Propiedades** , la casilla de verificación **Activar DLNA** está seleccionada de forma predeterminada. Desactive la casilla de verificación si desea deshabilitar la disponibilidad de DLNA.

A continuación, Añadir canales (en la página 434).

Añadir canales

Los dispositivos DLNA descubren los canales definidos en su sistema XProtect. Hay diferentes tipos de canales DLNA a los que puede asignar una cámara:

- Cámara única

  Una cámara por canal
- Ronda

  Múltiples cámaras por canal El canal cambia entre las cámaras seleccionadas en un intervalo de tiempo definido.
- Basado en reglas

  Una o varias cámaras por canal Las cámaras se configuran o eliminan del canal basado en reglas en función de los eventos.

Nota: Después de crear el canal, debe crear nuevas reglas en **Reglas** para mostrar las cámaras en este canal (ver "Añadir una regla" en la página 208).

Para seleccionar las cámaras disponibles para dispositivos DLNA, siga estos pasos:

1. Haga clic en el botón **Añadir canales**.
2. Seleccione un tipo de canal
3. Haga clic en el servidor y en los grupos de cámaras para expandirlos y seleccionar las cámaras que desee.

Para ajustar la duración y el orden de cada cámara en un canal de ronda:

1. Seleccione una cámara y ajuste la hora.
2. Use las flechas en la parte superior de la lista para cambiar el orden del ronda.

Para establecer la duración de la asignación de la cámara a un canal basado en reglas:

1. Seleccione la casilla de verificación **Retire la cámara del canal después**.
2. Establece el tiempo.

Los tipos de canales agregados aparecen en la **lista de canales**.

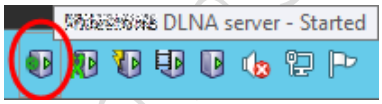
Administrar XProtect DLNA Server

Después de haber configurado XProtect DLNA Server, puede supervisar el servicio y cambiar la configuración de varias maneras.

Estado del servicio XProtect DLNA Server

Para ver el estado del servicio XProtect DLNA Server, siga estos pasos.

En el equipo donde está instalado el XProtect DLNA Server, busque en el área de notificación. El icono del XProtect DLNA Server Manager indica el estado del servicio XProtect DLNA Server con los siguientes colores:



- Verde: Ejecutando
- Amarillo: Comenzando o deteniéndose
- Rojo: Detenido

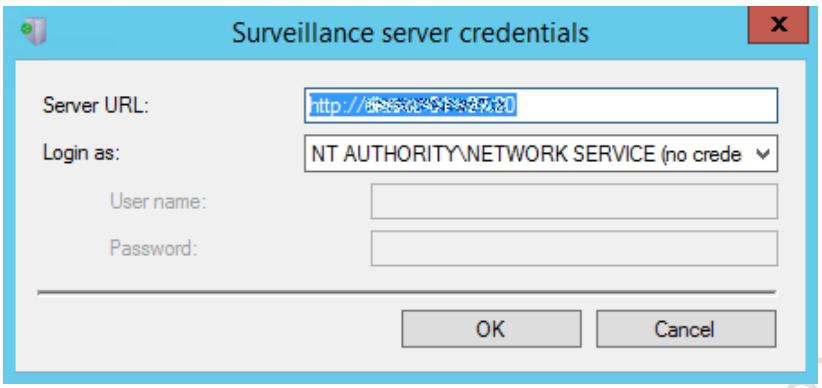
Si se detiene, haga clic con el botón derecho en el icono y seleccione **Iniciar XProtect DLNA Server**.

Cambiar las credenciales del servidor de vigilancia

Si cambia la dirección IP, el nombre de host, la cuenta de usuario o los números de puerto del servidor de vigilancia, debe actualizar esta información para XProtect DLNA Server. Los números de puerto para el XProtect DLNA Server también se pueden cambiar.

Para cambiar la dirección del servidor de gestión y las credenciales de inicio de sesión, siga estos pasos:

1. En la computadora donde está instalado el servicio XProtect DLNA Server, haga clic con el botón derecho en el icono de la bandeja del XProtect DLNA Server Manager y seleccione **Credenciales del servidor de vigilancia**.



2. Especifique la información nueva y haga clic en **OK**.

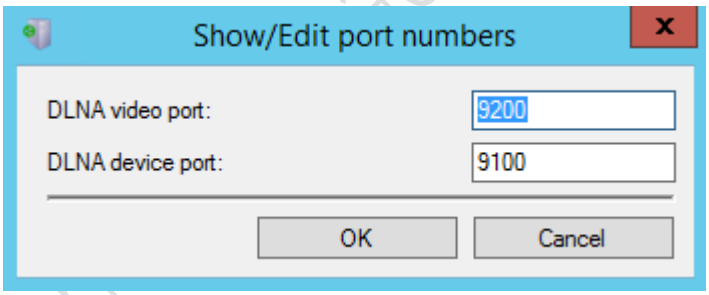
Nota: Debe utilizar el nombre de dominio o la dirección IP del servidor donde está instalado el servidor de gestión.

El servicio XProtect DLNA Server se reinicia y el icono de la bandeja se vuelve verde.

Editar números de puerto

Para cambiar los números de puerto XProtect DLNA Server, siga estos pasos:

1. En la computadora donde está instalado el servicio XProtect DLNA Server, haga clic con el botón derecho en el icono de la bandeja del XProtect DLNA Server Manager y seleccione **Mostrar / editar los números de puerto**.



2. Especifique la nueva información y, a continuación, haga clic en **Aceptar**.

El servicio XProtect DLNA Server se reinicia y el icono de la bandeja se vuelve verde.

Uso de un dispositivo certificado DLNA para ver secuencias de vídeo

Para empezar a ver vídeos en directo desde su sistema XProtect en sus pantallas públicas o TV, siga estos pasos:

1. Asegúrese de que su dispositivo esté certificado por DLNA y esté conectado a la red con XProtect DLNA Server.

2. Escanee la red y conéctela a XProtect DLNA Server cuando se ha descubierto.

Aparece una lista de los diferentes canales.

3. Conéctese al canal del que desea mostrar el video.
4. Verifica que el canal seleccionado muestre el video.

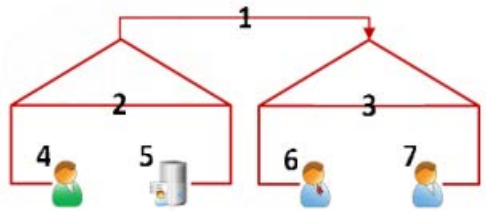
Multi-dominio con confianza unidireccional

Puesta en funcionamiento con confianza unidireccional

Si ejecuta su sistema en un entorno con varios dominios, puede configurar esta configuración con confianza unidireccional. El sistema está instalado en el dominio **confiando** y los usuarios se conectan desde dominios **confiandos** y **confiar**.

1. Cree una cuenta de servicio en el dominio **de confianza**. Puede darle el nombre que desee, por ejemplo, **svcMilestone**.
2. Añadir la nueva cuenta de servicio a los siguientes grupos locales de usuario de Windows en el servidor que ejecutan el sistema, en el dominio **confiar**:
   - Administradores
   - IISIUSRS (Windows Server 2008, necesaria para los servicios de Internet Information Server (IIS) Grupos de aplicaciones)
   - IISWPG (Windows Server 2003, necesario para IIS Grupos de aplicaciones).
3. Asegúrese de que la cuenta de servicio tiene derechos de administrador del sistema en su base de datos SQL o SQL Server Express, ya sea directamente oa través del grupo **BUILTIN\Administradors**.
4. Establecer la identidad de la **ManagementServerAppPool** grupo de aplicaciones en los IIS a la cuenta de servicio.
5. Reiniciar el servidor para asegurarse de que todos los cambios de pertenencia a grupos y permisos surtan efecto.

Importante: Para añadir usuarios de dominio **confiables** a funciones de sistema nuevas o existentes de XProtect, inicie sesión en Windows como un usuario de dominio **de confianza**. A continuación, inicie el Management Client e inicie sesión como usuario de **Confiado** dominio o el **Confiado** dominio. Si inicia sesión en Windows como **Confiado** usuario del dominio, se le solicitarán las credenciales **Confiado** dominio para buscar usuarios.



Ejemplo ilustración de entornos de varios dominios con confianza unidireccional:

1. Unidireccional saliente de dominio de confianza
2. MyDomain. local
3. OtherDomain.edu

4. Usuario dominio que confía
5. Servidor de gestión
6. Cuenta de servicio de Milestone
7. Usuario de dominio de confianza

SNMP

Soporte SNMP (explicado)

El sistema admite Simple Network Management Protocol (SNMP), un protocolo estándar para los dispositivos de seguimiento y control de la red, la gestión de su configuración, la recopilación de estadísticas y más.

El sistema actúa como un agente de SNMP, que puede generar una trampa SNMP, como resultado de una regla disparada. Una consola de administración SNMP de terceros a continuación, puede recibir información sobre el evento que activa la regla, y los operadores de la consola de gestión SNMP puede configurar su sistema para nuevas acciones si es necesario.

La implementación utiliza Microsoft® Windows® SNMP Service para activar trampas SNMP. Esto significa que se debe instalar el servicio SNMP en servidores de grabación. Cuando haya configurado el servicio SNMP a través de su propia interfaz de usuario, esto permite que los servidores de grabación para enviar archivos . mib (Management Information Base) a la consola de gestión SNMP.

Instalar el servicio SNMP

1. En los servidores de grabación pertinentes, abierta funcionalidad **Programas y características** de Windows.
2. En el lado izquierdo del cuadro de diálogo **Programas y funciones**, haga clic en **Active o desactive la funcionalidad de Windows**. Esto abre ventana **Disponen de Windows**.
3. En el cuadro de diálogo, seleccione la casilla de verificación junto a **Simple Network Management Protocol (SNMP)** y haga clic en **OK**.

Configurar servicio SNMP

1. En los servidores de grabación requeridas, seleccione **Inicio** > **Panel de control** > **Herramientas administrativas** > **Servicios**.
2. Haga doble clic en el servicio SNMP.
3. Seleccionar pestaña **Trampas**.
4. Especificar un nombre de comunidad, y haga clic en **Añadir a la lista**.
5. Seleccione los **destinos** pestaña.
6. Haga clic en **Añadir**, y especifique la dirección IP o nombre del servidor que ejecuta el software de terceros estación de gestión SNMP.
7. **Haga clic en OK (aceptar)**.

XProtect Professional VMS Servers

Servidores XProtect Professional VMS (explicados)

Esta sección sólo es relevante si:

- su sistema no utiliza IPv6, y
- tiene instalaciones con XProtect Professional VMS versión 7.0 o posterior.

En todos los demás casos, utilizar Milestone Federated Architecture o Milestone Interconnect.

Puede agregar servidores XProtect Professional VMS a su sistema XProtect VMS. Cuando se añade, los servidores actúan como servidores de grabación y su video se pueden ver por los clientes.

En el Management Client, puede ver el estado de los servidores XProtect Professional VMS añadidos. Debe definir todas las configuraciones del servidor XProtect Professional VMS (cámaras, programación, derechos de usuario, etc.) en Management Application de XProtect Professional VMS. Consulte la documentación XProtect Professional VMS.

Para que los usuarios tengan acceso a los videos de los servidores XProtect Professional VMS, deben coincidir los cometidos en XProtect VMS con los derechos de usuario definidos en los servidores XProtect Professional VMS.

- Agregar servidores (ver "Agregar servidores XProtect Professional VMS" en la página 440)XProtect Professional VMS
- Defina cometidos con acceso a (ver "Defina roles con acceso a servidores XProtect Professional VMS" en la página 441)XProtect Professional VMS servidores (ver "Defina roles con acceso a servidores XProtect Professional VMS" en la página 441)
- Editar servidores (ver "Edición de servidores XProtect Professional VMS" en la página 441)XProtect Professional VMS

Agregar servidores XProtect Professional VMS

Incluso si el sistema XProtect Professional VMS tiene una configuración interna de maestro / esclavo, no podrá reutilizarlo en su sistema XProtect VMS. Debe agregar cada servidor XProtect Professional VMS del que necesite datos de dispositivo individualmente.

Para agregar un servidor XProtect Professional VMS existente a su sistema:

1. En el menú **Herramientas** de Management Client, seleccione **Servidores Professional VMS**.
2. En el **Agregar / quitar Professional VMS Servidores** cuadro de diálogo, haga clic en **Agregar** .
3. Introduzca la dirección IP o el nombre de host del servidor XProtect Professional VMS.
4. Introduzca el número de puerto utilizado por el servidor XProtect Professional VMS.

   El número de puerto predeterminado es 80. Si tiene dudas, puede encontrar el número de puerto en Management Application de XProtect Professional VMS en **Acceso de servidor**.
5. Introduzca las credenciales de usuario para que el administrador del servidor XProtect Professional VMS pueda otorgarle derechos sin restricciones a los datos del dispositivo.

6. Si el sistema XProtect VMS accede al servidor XProtect Professional VMS a través de una conexión a Internet, haga clic en **Red** para especificar la dirección WAN del servidor de gestión de XProtect VMS. Sólo es necesario definir la dirección WAN una vez.

El siguiente paso es dar a sus usuarios acceso a los dispositivos desde el servidor XProtect Professional VMS.

Defina roles con acceso a servidores XProtect Professional VMS

Para que los usuarios accedan a dispositivos desde los servidores XProtect Professional VMS añadidos:

1. En el servidor XProtect Professional VMS, abra el Management Application para buscar un usuario XProtect Professional VMS que tenga derechos de usuario que pueda reutilizar y hacer coincidir con un rol en su sistema XProtect VMS. Si no, cree un nuevo XProtect Professional VMS usuario que coincida con el rol en su sistema XProtect VMS.
2. Tenga en cuenta el nombre de usuario del usuario XProtect Professional VMS, la contraseña y el tipo de autenticación (básico o Windows). El sistema XProtect VMS no verifica que la información que especifique más adelante en estos pasos corresponda a un usuario definido en XProtect Professional VMS.
3. En el panel **Navegación del sitio** XProtect VMS Management Client, expanda **Seguridad** y seleccione **Roles** .
4. Seleccione la función que desea utilizar o definir un nuevo cometido.
5. En la parte inferior del panel Configuración **de función** , seleccione la ficha **Servidores** y, a continuación, el servidor XProtect Professional VMS.
6. Seleccione el usuario XProtect Professional VMS con los derechos de usuario que desea que coincidan con su función.
7. **Haga clic en Guardar**.

Edición de servidores XProtect Professional VMS

Para editar un servidor XProtect Professional VMS añadido a su sistema:

1. En el menú **Herramientas** , seleccione **Professional VMS Servidores** .
2. Seleccione el servidor XProtect Professional VMS de la lista y haga clic en **Editar** .
3. Editar los ajustes pertinentes y haga clic en **OK**.

Mantenimiento del sistema

Puertos usados por el sistema

Todos XProtect componentes y los puertos necesarios por ellos se enumeran en secciones individuales a continuación. Para garantizar, por ejemplo, que el cortafuegos bloquea únicamente el tráfico no deseado, debe especificar los puertos que utiliza el sistema. Sólo debe habilitar estos puertos. Las listas también incluyen los puertos utilizados para los procesos locales.

Están dispuestos en dos grupos:

- **Los componentes del servidor** (servicios) ofrecen su servicio en determinados puertos, por lo que necesitan escuchar las peticiones de los clientes en estos puertos. Por lo tanto, estos puertos deben estar abiertos en Windows Firewall para las conexiones entrantes.
- **Componentes de cliente** (clientes) inician conexiones a puertos particulares en componentes de servidor. Por lo tanto, estos puertos necesitan ser abiertos para conexiones salientes. Conexiones de salida son normalmente abierta por defecto en el Firewall de Windows.

Si nada más se menciona, se deben abrir los puertos para componentes de servidor para las conexiones entrantes, y se deben abrir los puertos para componentes de cliente para conexiones salientes.

No tener en cuenta que los componentes del servidor pueden actuar como clientes a otros componentes del servidor también.

Los números de puerto son los números predeterminados, pero esto se puede cambiar. Póngase en contacto con Milestone Support, si es necesario cambiar los puertos que no se pueden configurar a través del Management Client.

Los componentes de servidor (conexiones entrantes)

Cada una de las secciones siguientes se enumeran los puertos que deben abrirse para un servicio particular. Con el fin de averiguar lo que necesitan ser abiertos en un equipo determinado puertos, debe tener en cuenta todos los servicios que se ejecutan en este equipo.

Servicio de Management Server y los procesos relacionados

Número de puerto	Protocolo	Procesamiento	Las conexiones desde...	Objetivo
80	HTTP	IIS	Todos los componentes XProtect	Comunicación principal, por ejemplo, la autenticación y configuraciones.
443	HTTPS	IIS	XProtect Smart Client y Management Client	La autenticación de los usuarios básicos.
6473	TCP	Servicio Management Server	Icono de la bandeja del Management Server Manager, conexión local solamente.	Que muestra el estado y la gestión del servicio.

Número de puerto	Protocolo	Procesamiento	Las conexiones desde...	Objetivo
7475	TCP	Servicio Management Server	Servicio Windows SNMP	La comunicación con el agente de extensión SNMP. No utilice el puerto para otros fines, incluso si su sistema no se aplica SNMP. En sistemas XProtect 2014 o mayores, el número de puerto era 6475.
8080	TCP	Servidor de gestión	Conexión local solamente.	La comunicación entre los procesos internos en el servidor.
9993	TCP	Servicio Management Server	Servicios Recording Server	La autenticación, la configuración, el intercambio simbólico.
12345	TCP	Servicio Management Server	XProtect Smart Client	La comunicación entre el sistema y los receptores de la Matrix. Se puede cambiar el número de puerto en el Management Client.

Servicio de SQL Server

Número de puerto	Protocolo	Procesamiento	Las conexiones desde...	Objetivo
1433	TCP	SQL Server	Servicio Management Server	Almacenamiento y recuperación de configuraciones.
1433	TCP	SQL Server	Servicio Event Server	Almacenamiento y recuperación de eventos.
1433	TCP	SQL Server	Servicio Log Server	Almacenamiento y recuperación de las entradas del registro.

Servicio de Data Collector

Número de puerto	Protocolo	Procesamiento	Las conexiones desde...	Objetivo
7609	HTTP	IIS	En el equipo del servidor de gestión: Servicios de Data Collector sobre todos los demás servidores. En otros equipos: Servicio Data Collector en el servidor de gestión.	Monitor de sistema.

Servicio Event Server

Número de puerto	Protocolo	Procesamiento	Las conexiones desde . . .	Objetivo
1234	TCP / UDP	Servicio Event Server	Cualquier servidor de envío de eventos genéricos a su sistema XProtect.	Detección de eventos genéricos de sistemas o dispositivos externos. Sólo si se habilita la fuente de datos pertinente.
1235	TCP	Servicio Event Server	Cualquier servidor de envío de eventos genéricos a su sistema XProtect.	Detección de eventos genéricos de sistemas o dispositivos externos. Sólo si se habilita la fuente de datos pertinente.
9090	TCP	Servicio Event Server	Cualquier sistema o dispositivo que envía evento analítico de su sistema XProtect.	La escucha de Eventos de Analytics de sistemas o dispositivos externos. Sólo es relevante si los eventos de analytics característica está habilitada.
22331	TCP	Servicio Event Server	XProtect Smart Client y Management Client	Los datos de configuración, eventos, alarmas, y el mapa.
22333	TCP	Servicio Event Server	MIP Plug-ins y aplicaciones.	MIP mensajería.

Servicio Recording Server

Número de puerto	Protocolo	Procesamiento	Las conexiones desde . . .	Objetivo
25	SMTP	Servicio Recording Server	Cámaras, codificadores y dispositivos de E / S.	La escucha de mensajes de eventos de dispositivos. El puerto está deshabilitado por defecto.
5210	TCP	Servicio Recording Server	Servidores de grabación failover.	Fusión de las bases de datos después de un servidor de grabación de conmutación por error había estado corriendo.
5432	TCP	Servicio Recording Server	Cámaras, codificadores y dispositivos de E / S.	La escucha de mensajes de eventos de dispositivos.
7474	TCP	Servicio Recording Server	Servicio Windows SNMP	La comunicación con el agente de extensión SNMP. No utilice el puerto para otros fines, incluso si su sistema no se aplica SNMP. En sistemas XProtect 2014 o mayores, el número de puerto era 6474.
7563	TCP	Servicio Recording Server	XProtect Smart Client, Management Client	Recuperando de vídeo y audio flujos, los comandos PTZ.
8966	TCP	Servicio Recording Server	Icono de la bandeja del Recording Server Manager, conexión local solamente.	Que muestra el estado y la gestión del servicio.
11000	TCP	Servicio Recording Server	Servidores de grabación Failover	Sondeo el estado de los servidores de grabación.
65101	UDP	Servicio Recording Server	Unica conexión local	La escucha de notificaciones de eventos de los controladores.

Tenga en cuenta que, además de las conexiones de entrada con el servicio Recording Server mencionadas anteriormente, el servicio Recording Server establece las conexiones salientes a las cámaras.

Servicio de Failover Server y el servicio de Failover Recording Server

Número de puerto	Protocolo	Procesamiento	Las conexiones desde . . .	Objetivo
25	SMTP	Servicio Recording Server	Cámaras, codificadores y dispositivos de E / S.	La escucha de mensajes de eventos de dispositivos. El puerto está deshabilitado por defecto.

Número de puerto	Protocolo	Procesamiento	Las conexiones desde . . .	Objetivo
5210	TCP	Servicio Recording Server	Servidores de grabación Failover	Fusión de las bases de datos después de un servidor de grabación de conmutación por error había estado corriendo.
5432	TCP	Servicio Recording Server	Cámaras, codificadores y dispositivos de E / S.	La escucha de mensajes de eventos de dispositivos.
7474	TCP	Servicio Recording Server	Servicio Windows SNMP	La comunicación con el agente de extensión SNMP. No utilice el puerto para otros fines, incluso si su sistema no se aplica SNMP.
7563	TCP	Servicio Recording Server	XProtect Smart Client	Recuperando de vídeo y audio flujos, los comandos PTZ.
8844	UDP	Servidores de grabación Failover	Conexión local solamente.	La comunicación entre los servidores.
8966	TCP	Servicio Failover Recording Server	Icono de la bandeja del Failover Recording Server Manage, conexión local solamente.	Que muestra el estado y la gestión del servicio.
8967	TCP	Servicio Failover Server	Icono de la bandeja de Failover Server Manager, conexión local solamente.	Que muestra el estado y la gestión del servicio.
8990	TCP	Servicio Failover Server	Servicio Management Server	Supervisión del estado del servicio Failover Server.

Tenga en cuenta que, además de las conexiones de entrada con el servicio Failover Recording Server mencionadas anteriormente, el servicio de grabación de servidor establece las conexiones salientes a las cámaras.

Servicio Mobile Server

Número de puerto	Protocolo	Procesamiento	Las conexiones desde . . .	Objetivo
8000	TCP	Servicio Mobile Server	Icono de la bandeja de Mobil Server Manager, conexión local solamente.	Aplicación SysTray.
8081	HTTP	Servicio Mobile Server	Clientes Mobile, los clientes Web y Management Client.	Envío de flujos de datos; de vídeo y audio.

Número de puerto	Protocolo	Procesamiento	Las conexiones desde . . .	Objetivo
8082	HTTPS	Servicio Mobile Server	Clientes Mobile y clientes Web.	Envío de flujos de datos; de vídeo y audio.

Servicio LPR Server

Número de puerto	Protocolo	Procesamiento	Las conexiones desde . . .	Objetivo
22334	TCP	Servicio LPR Server	Servidor de eventos	Recuperando placas de circulación reconocidos y el estado del servidor. Para conectarse, el servidor de eventos debe tener instalado el complemento LPR.
22334	TCP	Servicio LPR Server	Icono de la bandeja de LPR Server Manager, conexión local solamente.	Aplicación de SysTray

Servicio Milestone ONVIF Bridge

Número de puerto	Protocolo	Procesamiento	Las conexiones desde...	Objetivo
580	TCP	Servicio ONVIF Bridge	Clientes ONVIF	Autenticación y solicitudes de configuración de flujo de vídeo.
554	RTSP	Servicio RTSP	Clientes ONVIF	Transmisión de vídeo solicitado a los clientes de ONVIF.

Servicio XProtect DLNA Server

Número de puerto	Protocolo	Procesamiento	Las conexiones desde...	Objetivo
9100	HTTP	Servicio DLNA Server	Dispositivo DLNA	Detección de dispositivos y configuración de canales DLNA. Solicitud de secuencias de vídeo.
9200	HTTP	Servicio DLNA Server	Dispositivo DLNA	Transmisión de vídeo solicitado a dispositivos DLNA.

Servicio Screen Recorder

Número de puerto	Protocolo	Procesamiento	Las conexiones desde . . .	Objetivo
52111	TCP	XProtect Screen Recorder	Servicio Recording Server	Proporciona vídeo de un monitor. Parece y actúa de la misma manera como una cámara en el servidor de grabación. Se puede cambiar el número de puerto en el Management Client.

Cámaras, codificadores, y los dispositivos de E / S

Conexiones entrantes

Número de puerto	Protocolo	Las conexiones desde...	Objetivo
80	TCP	Servidores de grabación y servidores de grabación de conmutación por error	Autenticación, la configuración y flujos de datos; de vídeo y audio.
443	HTTPS	Servidores de grabación y servidores de grabación de conmutación por error	Autenticación, la configuración y flujos de datos; de vídeo y audio.
554	RTSP	Servidores de grabación y servidores de grabación de conmutación por error	Los flujos de datos; de vídeo y audio.

Las conexiones salientes

Número de puerto	Protocolo	Conexiones para...	Objetivo
25	SMTP	Servidores de grabación y servidores de grabación de conmutación por error	Envío de notificaciones de eventos (en desuso).
5432	TCP	Servidores de grabación y servidores de grabación de conmutación por error	El envío de notificaciones de eventos.

Tenga en cuenta que sólo unos pocos modelos de cámaras son capaces de establecer conexiones salientes.

Los componentes de cliente (conexiones salientes)

XProtect Smart Client, XProtect Management Client, Milestone Mobile servidor

Número de puerto	Protocolo	Conexiones para...	Objetivo
80	HTTP	Servicio Management Server	Autenticación
443	HTTPS	Servicio Management Server	La autenticación de los usuarios básicos.
7563	TCP	Servicio Recording server	Recuperando de vídeo y audio flujos, los comandos PTZ.
22331	TCP	Servicio Event Server	Alarmas.

Web Client, Milestone Mobile cliente

Número de puerto	Protocolo	Conexiones para...	Objetivo
8081	HTTP	Servidor Milestone Mobile	Recuperando flujos de vídeo y audio.
8082	HTTPS	Servidor Milestone Mobile	Recuperando flujos de vídeo y audio.

Copia de seguridad y restauración de la configuración del sistema

Copia de seguridad y restauración de la configuración del sistema (explicado)

Milestone recomienda que haga copias de seguridad de la configuración del sistema como medida de recuperación de desastres. Si bien es raro que perder su configuración, puede suceder en circunstancias desafortunadas. Afortunadamente, respaldar su configuración actual se puede hacer en cuestión de minutos.

El sistema ofrece una función incorporada que realiza copias de toda la configuración del sistema se pueden definir en el Management Client. Tenga en cuenta que la base de datos del servidor de registro y los archivos de registro, incluyendo los archivos de registro de auditoría, no están incluidos en esta copia de seguridad.

Si el sistema es grande, Milestone recomienda que defina copias de seguridad programadas. Esto se hace con la herramienta de terceros: Microsoft® SQL Server Management Studio . Esta copia de seguridad incluye los mismos datos que una copia de seguridad manual.

Durante una copia de seguridad, su sistema permanece en línea.

Copia de seguridad de la configuración de su sistema puede llevar algo de tiempo. La duración de la copia de seguridad depende de:

- la configuración de tu sistema
- su hardware, y en
- si ha instalado el servidor SQL, el servicio del servidor de eventos y el Management Client en un solo servidor o en varios servidores.

Cada vez que realice una copia de seguridad manual y programada, un archivo de registro de transacciones de SQL Server de la se vacía. Para obtener información adicional acerca de cómo vaciar este archivo de registro, vaya al sitio web de Microsoft y busque "Registro de transacciones de SQL Server"/"SQL Server transaction log.".

Copia de seguridad de base de datos de servidor de registro

Maneje la base de datos **SurveillanceLogServer** utilizando el método que utiliza al manejar la configuración del sistema como se describió anteriormente. La base de datos **SurveillanceLogServer** (el nombre puede ser diferente si ha cambiado el nombre a la base de datos de configuración del sistema) contiene todos los registros del sistema, incluidos los errores registrados por los servidores de grabación y las cámaras.

La base de datos se encuentra donde está instalado el servidor SQL del servidor de registro, por lo general el mismo lugar que el servidor SQL de su servidor de gestión. Copia de seguridad de esta base de datos no es vital, ya que no contiene ninguna configuración del sistema, pero puede apreciar que después han tenido acceso a los registros del sistema de copia de seguridad antes de que el servidor de gestión / restauración.

Copia de seguridad manual y restauración de la configuración del sistema

Copia de seguridad manual de la configuración del sistema (explicada)

Cuando se desea realizar una copia de seguridad manual de la configuración del sistema, asegúrese de que su sistema se mantiene en línea. Aquí hay algunas cosas a considerar antes de iniciar la copia de seguridad:

- No se puede utilizar una copia de seguridad para copiar configuraciones para otros sistemas.
- Puede tomar algún tiempo para copia de seguridad de su configuración. Depende de la configuración del sistema, el hardware, y de si el servidor SQL, Management Client y gestión de cliente están instalados en el mismo equipo.
- Troncos, incluidos los registros de auditoría, **no** son parte de la copia de seguridad de configuración.

Copia de seguridad y restauración de la configuración del servidor de eventos (explicado)

El contenido de la configuración del servidor de eventos se incluye al realizar una copia de seguridad y restaurar la configuración del sistema.

La primera vez que se ejecuta el servidor de eventos, todos sus archivos de configuración se mueven automáticamente al servidor SQL. Puede aplicar la configuración restaurada al servidor de eventos sin necesidad de reiniciar el servidor de eventos, y el servidor de eventos puede iniciar y detener todas las comunicaciones externas mientras se carga la restauración de la configuración.

Escenarios de fallos y problemas de copia de seguridad y restauración (explicado)

Si, después de la copia de seguridad de configuración último sistema, se ha mudado al servidor de eventos u otros servicios registrados tales como el servidor de registro, debe seleccionar la que ha registrado la configuración del servicio que desea para el nuevo sistema. Puede decidir mantener la nueva configuración

después de que el sistema se restaura a la versión anterior. Usted decide examinado los nombres de host de los servicios.

Si su restauración de la configuración del sistema falla porque el servidor de eventos no se encuentra en el destino especificado (por ejemplo, si ha elegido la configuración de servicio registrada de edad), hacer otra restauración.

Copias de seguridad de la configuración del sistema de forma manual

1. Desde la barra de menús, seleccione **Archivo** > **configuración de respaldo**.
2. Lea la nota en el cuadro de diálogo y haga clic en **Copia de seguridad**.
3. Introduzca un nombre de archivo para el archivo .cnf.
4. Introduce un destino de carpeta y haga clic en **Guardar**.
5. Espere hasta que finalice la copia de seguridad y haga clic en **Cerrar**.

Nota: Todos los archivos de configuración del sistema relevantes se combinan en un solo archivo . cnf único que se guarda en una ubicación especificada. Durante la copia de seguridad, todos los archivos de copia de seguridad se exportan primero en una carpeta de copia de seguridad temporal del sistema en el servidor de gestión. Se puede seleccionar otra carpeta temporal, haga clic en el icono de servicio del servidor de gestión del área de notificación de y seleccionando Seleccionar carpeta de copia de seguridad compartida.

Restauración de la configuración del sistema desde una copia de seguridad manual

Información importante:

- El usuario que instala y el usuario que restaura debe ser administrador local de la base de datos en el servidor de gestión **y** en el servidor SQL.
- A excepción de sus servidores de grabación, el sistema está completamente cerrado por la duración de la restauración, que puede llevar algún tiempo.
- Una copia de seguridad sólo puede ser restaurada en la instalación del sistema en el que se ha creado. Asegúrese de que la configuración es lo más similar posible a la que se realizó la copia de seguridad. De lo contrario, la restauración falle.
- Si usted hace una copia de seguridad de la base de datos y restaurar en un servidor SQL limpia, entonces los errores de subida desde la base de datos no funcionarán y sólo recibirán un mensaje de error genérico desde el servidor SQL. Para evitar esto, vuelva a instalar primero el sistema XProtect utilizando el servidor SQL limpia y luego restaurar la copia de seguridad por encima de eso.
- Si la restauración falla durante la fase de validación, puede iniciar la configuración antigua de nuevo, ya que han hecho cambios.
  Si falla la restauración de otras partes en el proceso, no se puede volver a utilizar la configuración antigua.
  Mientras el archivo de copia de seguridad no está dañado, se puede hacer otra restauración.
- La restauración sustituye a la configuración actual. Esto significa que cualquier cambio en la configuración de copia de seguridad desde la última se pierden.
- No hay registros, incluyendo los registros de auditoría, se restauran.
- Una vez que ha comenzado la restauración, no se puede cancelar.

La restauración:

1. Haga clic en el icono de servicio del servidor de gestión del área de notificación y seleccione de **restauración de la configuración**.
2. Lea la nota importante y haga clic en **Restaurar**.
3. En el cuadro de diálogo Abrir archivo, busque la ubicación del archivo de copia de seguridad de configuración, seleccione y haga clic en **Abrir**.

   El archivo de copia de seguridad se encuentra en el equipo de Management Client. Si el Management Client se instala en un servidor diferente, copiar el archivo de copia de seguridad a este servidor antes de seleccionar el destino.

4. Se abre la ventana **Restaurar configuración**. Espere a que la restauración hasta el final y haga clic en **Cerrar**.

Seleccione la carpeta de copia de seguridad compartida

Antes de realizar copias de seguridad y restaurar cualquier configuración de sistema, debe configurar una carpeta de copia de seguridad para este fin.

1. Haga clic en el icono de servicio del servidor de gestión del área de notificación y seleccione del **Seleccionar carpeta de copia compartida**.
2. En la ventana que aparece, vaya a la ubicación del archivo deseado.
3. Haga clic **OK** dos veces.
4. Si se le pregunta si desea eliminar los archivos en la carpeta de copia de seguridad actual, haga clic en **Sí** o **No** dependiendo de sus necesidades

Programada de copia de seguridad y restauración

Copia de seguridad programada y restauración de la configuración del sistema (explicado)

Milestone recomienda que haga copias de seguridad de la configuración del sistema como medida de recuperación de desastres. Si bien es raro que perder su configuración, puede suceder en circunstancias desafortunadas. Por suerte, sólo se necesita un minuto para copia de seguridad de la configuración existente. Copias de seguridad periódicas también tienen la ventaja añadida de que echar registro de transacciones de su Microsoft® SQL Server.

Si usted tiene una configuración más pequeña y no necesita copias de seguridad programadas, puede realizar copias de seguridad de la configuración del sistema de forma manual. Para obtener instrucciones, consulte Copia de seguridad manual y restauración de la configuración del sistema (en la página 450).

El servidor de gestión almacena la configuración del sistema en una base de datos. Cuando una copia de seguridad / servidor (s) de gestión de restauración, asegúrese de que esta base de datos está incluido en la copia de seguridad / restauración.

Requisitos para el uso de copia de seguridad y restauración programadas

Microsoft® SQL Server Management Studio, una herramienta de descarga-poder de forma gratuita desde su página web (http://www.microsoft.com/downloads).

Además de la gestión de bases de datos SQL Server, la herramienta incluye algunas de las características de copia de seguridad y restauración de fácil uso. Descargar e instalar la herramienta en el servidor de gestión.

Registro de transacciones del servidor SQL (explicado)

Cada vez que un cambio en los datos del sistema se produce, el SQL Server ingrese este cambio en su registro de transacciones, sin importar si se trata de un SQL Server en la red o una edición de SQL Server Express.

El registro de transacciones es esencialmente una función de seguridad que hace que sea posible para hacer retroceder y deshacer los cambios en la base de datos SQL Server. Por defecto, el servidor SQL Server almacena su registro de transacciones de forma indefinida, y con el tiempo el registro de transacciones se acumulan más y más entradas. El registro de transacciones de SQL Server está situado por defecto en la unidad del sistema, y si el registro de transacciones sigue creciendo, es posible que en el extremo impedir que Windows se ejecute correctamente.

Para evitar este escenario, el lavado de registro de transacciones de SQL de servir de vez en cuando es una buena idea. Sin embargo, el lavado no conlleva por sí mismo el archivo de registro de transacciones más pequeñas, pero impide que vuelva a crecer fuera de control. Su sistema no significa, sin embargo, a eliminar automáticamente el registro de transacciones de SQL Server a intervalos específicos. También se puede hacer varias cosas en el propio SQL Server para mantener el tamaño del registro de transacciones hacia abajo.

Para obtener más información sobre este tema, vaya a la página de soporte de Microsoft (http://support.microsoft.com) y la búsqueda de registro de transacciones de SQL Server.

Copia de seguridad de la configuración del sistema con la copia de seguridad programada

1. Desde el menú '**Inicio** de Windows, inicie Microsoft ® SQL Server Management Studio.
2. En la conexión, especifique el nombre del servidor SQL Server requerido. Usar la cuenta con la que se creó la base de datos.
    1. Encuentra la base de datos **Vigilancia** que contiene la configuración de todo el sistema, incluyendo el servidor de eventos, servidores de grabación, cámaras, entradas, salidas, usuarios, reglas, patrullando perfiles, etc.

        Suponemos que la base de datos utiliza el nombre predeterminado.
    2. Hacer una copia de seguridad de la base de datos de **vigilancia** y asegúrese de que:

    - Compruebe que la base de datos seleccionada es **Vigilancia**.
    - Compruebe que el tipo de copia de seguridad **completa** es.
    - Establecer la programación de la copia de seguridad recurrente. Puede leer más acerca de las copias de seguridad programadas y automatizadas en el sitio web de Microsoft (https://support.microsoft.com/en-us/kb/2019698).
    - Compruebe que la ruta sugerida es satisfactorio o seleccionar camino alternativo.
    - Seleccione para **verificar copia de seguridad cuando haya terminado** y para **realizar la suma de comprobación antes de escribir en los medios de comunicación** .

    3. Siga las instrucciones de la herramienta hasta el final.

También considerar la copia de seguridad de la base de datos **SurveillanceLog** utilizando el mismo método.

Copias de seguridad y restauración de la configuración del servidor de eventos

El contenido de la configuración del servidor de eventos se incluye al realizar una copia de seguridad y restaurar la configuración del sistema. La primera vez que se ejecuta el servidor de eventos, todos sus archivos de configuración se mueven automáticamente al servidor SQL. Puede aplicar la configuración restaurada al servidor de eventos sin necesidad de reiniciar el servidor de eventos, y el servidor de eventos es capaz de iniciar y detener todas las comunicaciones externas mientras se carga la restauración de la configuración.

Recuperación de la configuración del sistema desde una copia de seguridad programada

Requisitos
Para evitar cambios de configuración se realizan mientras se restaura la base de datos de configuración del sistema, detenga el:

- Servicio Management server (ver "Servicios Managing server" en la página 462)
- Servicio de servidor de eventos (se puede hacer desde Windows **Servicios** (busque **services.msc** en su equipo. Dentro **Servicios**, busque **Milestone XProtect Event Server**))
- Servicio de publicación World Wide Web , también conocido como el Servicio de Información de Internet (IIS). Información sobre cómo detener el IIS (http://technet.microsoft.com/en-us/library/cc732317(WS.10).aspx).

Abra Microsoft® SQL Server Management Studio desde Windows **inicio menú**.

En la herramienta de hacer lo siguiente:

1. En la conexión, especifique el nombre del servidor SQL Server requerido. Usar la cuenta en la que se ha creado la base de datos.
2. Encuentra la base de datos **Vigilancia** que contiene la configuración de todo el sistema, incluyendo el servidor de eventos, servidores de grabación, cámaras, entradas, salidas, usuarios, reglas, patrullando perfiles, etc.
3. Hacer una restauración de la **Vigilancia** base de datos y asegúrese de:
   - Seleccione una copia de seguridad **del** dispositivo
   - Seleccione el tipo **de archivo** de medio de copia de seguridad
   - Buscar y seleccionar el archivo de copia de seguridad **Surveillance.bak**
   - Seleccionar al **sobrescribir la base de datos existente**.
4. Siga las instrucciones de la herramienta hasta el final.

Si también copia de seguridad de la **SurveillanceLog** base de datos desde el servidor de registro antiguo, restaurarla en el nuevo servidor de registro utilizando el mismo método.

Tenga en cuenta que el sistema no funciona, mientras que el servicio Management Server se detiene. Es importante recordar para iniciar los servicios de nuevo una vez que haya terminado la restauración de la base de datos.

Al mover el servidor de gestión

Mover el servidor de administración (explicado)

A veces puede que tenga que mover la instalación del servidor de gestión de un servidor físico a otro. El servidor de gestión almacena la configuración del sistema en una base de datos. Si va a mover el servidor de gestión de un servidor físico a otro, es vital que se asegure de que su nuevo servidor de gestión también tiene acceso a esta base de datos. La base de datos de la configuración del sistema puede almacenarse de dos formas distintas:

- **Red de SQL Server:** Si va a guardar la configuración del sistema en una base de datos en un servidor SQL Server existente en su red, puede apuntar a la ubicación de la base de datos de SQL Server que al

instalar el software de servidor de gestión en su nuevo servidor de gestión. En ese caso, sólo el siguiente párrafo sobre el nombre de host del servidor de gestión y la dirección IP se aplica y se debe pasar por alto el resto de este tema:

Nombre de host y dirección IP del servidor de administración: Cuando se mueve el servidor de gestión de un servidor físico a otro servidor físico, es, con mucho, el más fácil de dar al nuevo servidor del mismo nombre de host y la dirección IP que el anterior. Esto es debido al hecho de que el servidor de grabación se conecta a la dirección IP y nombre de host del servidor de gestión de edad. Si usted ha dado el nuevo servidor de gestión de un nuevo nombre de host y / o la dirección IP, el servidor de impresión no puede encontrar el servidor de gestión. Detener manualmente cada servidor de grabación en el sistema, cambiar su dirección URL del servidor de gestión, y cuando se hace, reiniciarlos.

- **SQL Server local:** Si va a guardar la configuración del sistema en una base de datos de SQL Server local en el propio servidor de gestión, es importante realizar copias de seguridad de datos de configuración del sistema del servidor de gestión existente antes del movimiento. Por copias de seguridad de la base de datos, y posteriormente restaurarlo en el nuevo servidor, se evita tener que volver a configurar las cámaras, reglas, perfiles temporales, etc. después del movimiento.

Requisitos

- **El archivo de instalación de software para la instalación en el nuevo servidor de gestión .**
- **Su archivo de licencia de software (.lic)**, que recibió cuando compró su sistema y lo instaló inicialmente. No se debe utilizar el archivo de licencia de software activado por el que ha recibido después de una activación manual de la licencia fuera de línea. Un archivo de licencia de software activado contiene información sobre el servidor específico en el que está instalado el sistema. Por lo tanto, un archivo de licencia de software activado no se puede reutilizar cuando se mueve a un nuevo servidor.

Tenga en cuenta que si usted también está actualizando el software del sistema en relación con el movimiento, que ha recibido un nuevo archivo de licencia de software. Sólo tiene que utilizar esto.

- **Usuarios locales de SQL Server solamente: Microsoft® SQL Server Management Studio**.
- ¿Lo que sucede mientras el servidor de gestión no está disponible? (ver "Servidores de administración no disponibles (explicado)" en la página 455)
- Copiar la base de datos del servidor de registro (ver "Copia de seguridad de base de datos de servidor de registro" en la página 450)

Servidores de administración no disponibles (explicado)

- **Los servidores de grabación todavía pueden grabar:** Cualquier servidor de grabación que actualmente trabajan recibieron una copia de la configuración del servidor de gestión, para que puedan trabajar y almacenar las grabaciones por su cuenta, mientras que el servidor de gestión está abajo. Programado y funciona por detección de movimiento de grabación, por lo tanto, y de hecho provocó fábrica de grabación a menos basado en eventos relacionados con el servidor de gestión o cualquier otro servidor de grabación ya que estos pasan por el servidor de gestión.
- **Los servidores de grabación almacenan temporalmente los datos de registro localmente:** Ellos envían automáticamente datos de registro en el servidor de gestión cuando esté disponible de nuevo.
    - **Los clientes no pueden ingresar:** El acceso de cliente está autorizado a través del servidor de gestión. Sin el servidor de gestión, los clientes no pueden conectarse.

- **Los clientes que ya están logueados pueden permanecer identificados hasta por una hora:** Cuando los clientes se registran, son autorizadas por el servidor de gestión y se pueden comunicar con servidores de grabación para un máximo de una hora. Si usted puede conseguir el nuevo servidor de gestión en funcionamiento dentro de una hora, muchos de los usuarios no se ven afectados.
- **No se puede configurar el sistema:** Sin el servidor de gestión, no se puede cambiar la configuración del sistema.

Milestone recomienda que se informe a los usuarios sobre el riesgo de perder el contacto con el sistema de vigilancia, mientras que el servidor de gestión está abajo.

Mover la configuración del sistema

Traslado de la configuración del sistema es un proceso de tres pasos:

1. Hacer una copia de seguridad de la configuración del sistema. Esto es idéntico a hacer una copia de seguridad programada (ver "Copia de seguridad de la configuración del sistema con la copia de seguridad programada" en la página 453).
2. Instalar el nuevo servidor de gestión en el nuevo servidor. Ver copia de seguridad programada, el paso 2.
3. Restaura la configuración del sistema para el nuevo sistema. Ver restauración de la configuración del sistema de copia de seguridad programada (ver "Recuperación de la configuración del sistema desde una copia de seguridad programada" en la página 454).

Administrar el servidor SQL

Actualización de la dirección del servidor SQL (explicada)

Al instalar un sistema como un ensayo, o si la reestructuración de una gran instalación, puede que tenga que utilizar una base de datos SQL diferente. Puede hacer esto con la herramienta **Update SQL Server Address**.

Con la herramienta, puede cambiar las direcciones de los servidores SQL utilizadas por el servidor de gestión, el servidor de eventos y el servidor de registro. La única limitación es que no se puede cambiar el servidor de gestión y dirección de evento de SQL Server al mismo tiempo que la dirección SQL del servidor de registro. Puede hacerlo una tras otra.

Debe realizar actualizaciones SQL localmente en el equipo en el que ha instalado el servidor de administración / servidor de eventos **o** el servidor de registro. No se puede hacer desde el Management Client. Si el servidor de gestión y el servidor de eventos no se encuentran en el mismo equipo, puede seguir utilizando la herramienta, pero hay que ejecutarlo en tanto el equipo en el que está instalado el servidor de gestión y en el equipo en el que está instalado el servidor de eventos.

Debe copiar las bases de datos SQL antes de continuar.

Actualizar la dirección SQL del servidor de registro

Servidor de gestión y servidor de registro ubicado en el mismo equipo

1. Ir a la computadora donde está instalado el servidor de gestión.
2. Ir al área de notificación de la barra de tareas. Haga clic en el icono del **servidor de gestión**, seleccione **actualizar la dirección SQL**.Aparece el cuadro de diálogo **Actualización de dirección del servidor SQL**.
3. Seleccionar **Log Server** y haga clic en **Siguiente**.
4. Introducir o seleccionar el nuevo servidor SQL y haga clic en **Siguiente**.
5. Seleccione la nueva base de datos SQL y haga clic en **Seleccionar**.
6. Espere a que el cambio de dirección se lleva a cabo. Haga clic en **OK** para confirmar.

Servidor de gestión y el servidor de registro ubicado en equipos diferentes

1. Vaya al equipo donde está instalado su servidor de administración y copie el directorio %ProgramFiles%\Milestone\XProtect Management Server\Tools\ChangeSqlAddress\ (con contenido) en un directorio temporal del servidor de eventos.
2. Pegue el directorio que copió a un lugar temporal en el equipo donde está instalado el servidor de registro y ejecute el archivo incluido: VideoOS.Server.ChangeSqlAddress.exe. Aparece el cuadro de diálogo **Actualización de dirección del servidor SQL**.
3. Seleccionar **Log Server** y haga clic en **Siguiente**.
4. Introducir o seleccionar el nuevo servidor SQL y haga clic en **Siguiente**.
5. Seleccione la nueva base de datos SQL y haga clic en **Seleccionar**.
6. Espere a que el cambio de dirección se lleva a cabo. Haga clic en **OK** para confirmar.

Actualización de la dirección del servidor SQL servidor de gestión o servidor de eventos

1. Si el servidor de gestión y el servidor de eventos se encuentran:
    1. juntos en el mismo equipo y desea actualizar ambas direcciones SQL, ir a la computadora donde está instalado el servidor de gestión.
    2. en equipos diferentes y desea actualizar la dirección de administración de SQL Server (y más tarde la dirección SQL servidor de eventos), ir a la computadora donde está instalado el servidor de gestión.
    3. en equipos diferentes y desea actualizar solo la dirección SQL del servidor de eventos (o ya la ha actualizado en el servidor de administración), vaya a la computadora donde está instalado su servidor de administración y copie el directorio %ProgramFiles%\Milestone\XProtect Management Server\Tools\ChangeSqlAddress\ (con contenido) al directorio temporal en el servidor de eventos.
2. Si tu eliges:

1. pasos **1.1** y **1.2**, vaya al área de notificación de la barra de tareas. Haga clic en el icono del **servidor de gestión**, seleccione **actualizar la dirección SQL**. Repita el proceso para actualizar la dirección del servidor de eventos SQL.

2. paso **1.3**,pegue el directorio que copió en un lugar temporal en la computadora donde está instalado el servidor de eventos y ejecute el archivo incluido:VideoOS.Server.ChangeSqlAddress.exe.

3. Aparece el cuadro de diálogo **actualización de dirección del servidor SQL**. Seleccionar **servidor de gestión y Servidor de eventos** y haga clic **Siguiente**.

4. Introducir o seleccionar el nuevo servidor SQL y haga clic en **Siguiente**.

5. Seleccione la nueva base de datos SQL y haga clic en **Seleccionar**.

6. Espere a que el cambio de dirección se lleva a cabo. Cuando se presenta un mensaje de confirmación, haga clic en **OK**.

Reemplazar el hardware

Cuando se sustituye un dispositivo de hardware de la red con otro dispositivo de hardware, debe conocer la dirección IP, puerto, nombre de usuario y la contraseña del nuevo dispositivo de hardware.

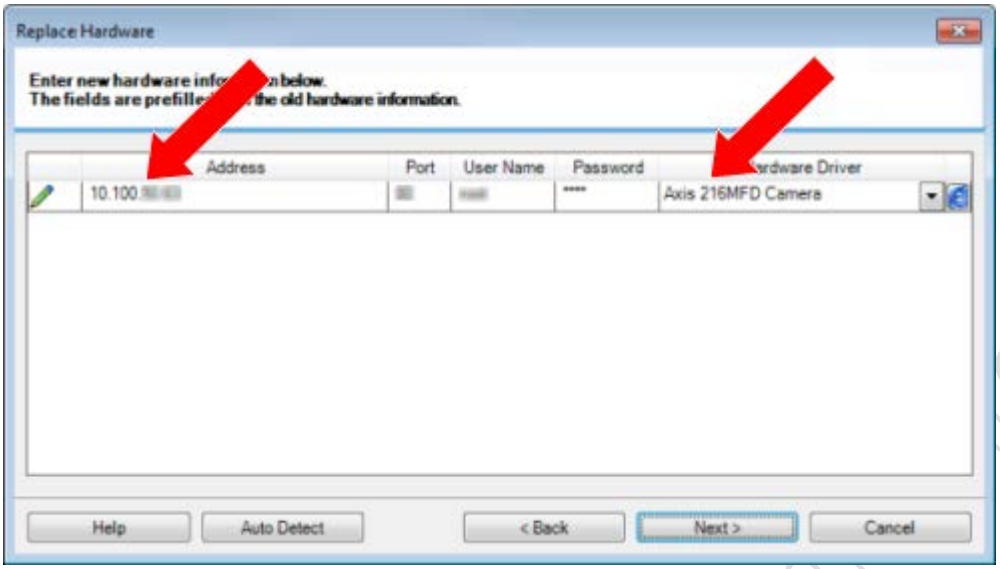
Si no ha habilitado activación de licencia automática (ver "Activación automática de la licencia (explicada)" en la página 75) y ha utilizado todos los cambios de dispositivo sin activación (ver "Cambios de dispositivo sin activación (explicado)" en la página 73), debe activar manualmente sus licencias **después de** en sustitución de dispositivos de hardware.Si el nuevo número de dispositivos de hardware supera el número total de licencias de dispositivos de hardware, usted tiene que comprar nuevas licencias de dispositivos de hardware.

1. Expanda el servidor de grabación deseada, haga clic en el hardware que desea reemplazar.

2. Seleccionar **reemplazar el hardware**.

3. Aparecerá el asistente para **reemplazar hardware**.Haga clic en **Siguiente**.

4. En el asistente, en el campo **Dirección** (marcado con una flecha roja en la imagen), introduzca la dirección IP del nuevo hardware.Si se conoce, seleccione el controlador correspondiente en la lista desplegable Hardware **Hardware Driver**.De lo contrario seleccione **Detección automática**.Si el puerto, nombre de usuario o contraseña de los datos es diferente para el nuevo hardware, corregir este **antes de iniciar el proceso de auto detectar (si es necesario)**.



El asistente se llena previamente con los datos del hardware existente. Si se sustituya por un dispositivo de hardware similar, se puede volver a utilizar algunos de estos datos - por ejemplo, el puerto y la información para el controlador.

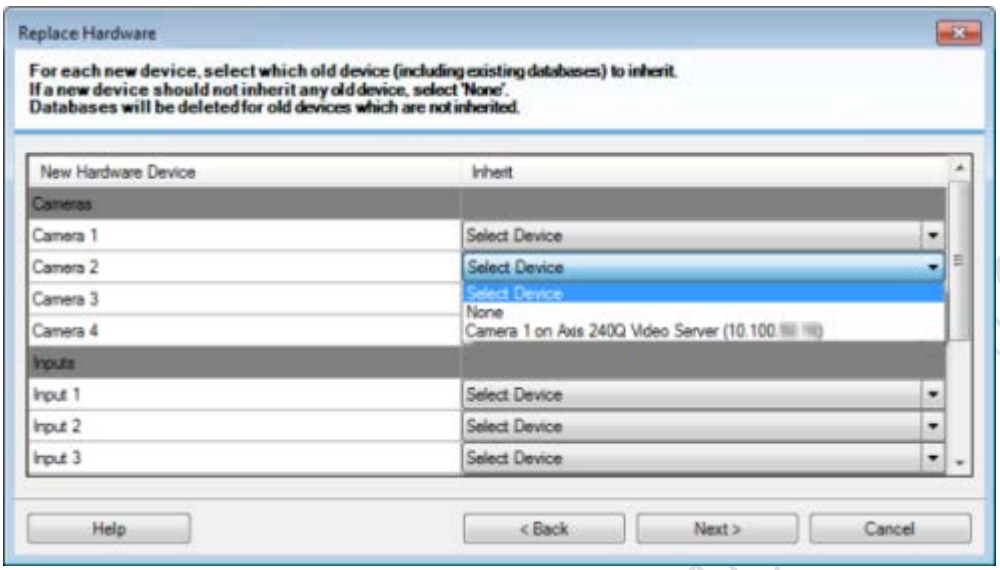
5. Puede seguir estos pasos:

   - Si ha seleccionado el controlador de dispositivo de hardware solicitado a través de la lista, haga clic en **Siguiente**.
   - Si seleccionó **Detección automática** en la lista, haga clic en **Detección automática**, espere a que este proceso tenga éxito (marcado con un ✔ a la izquierda), haga clic en**Siguiente**.

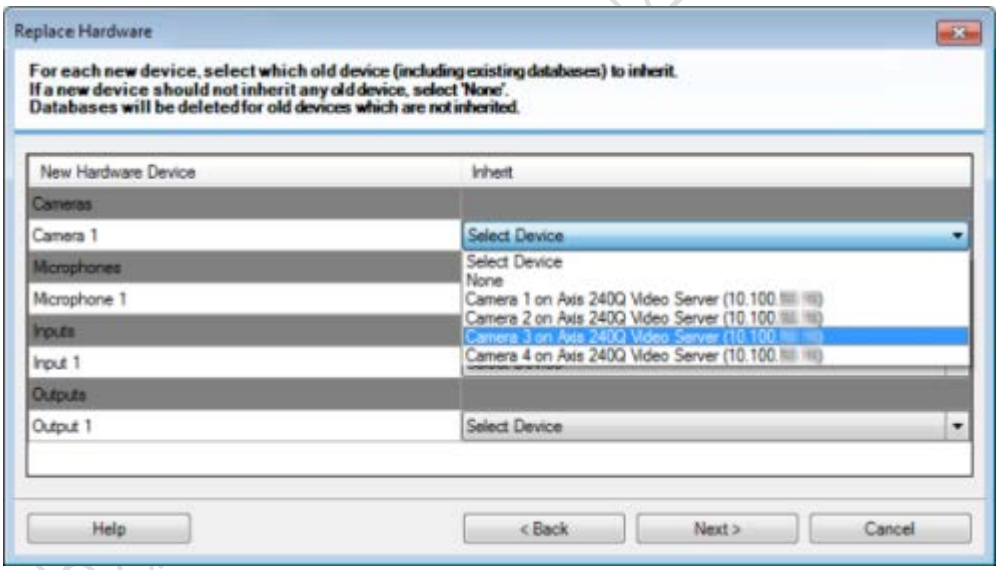
   Este paso está diseñado para ayudarle a trazar los dispositivos y sus bases de datos, dependiendo del número de cámaras, micrófonos individuales, entradas, salidas, etc. unida al dispositivo de hardware antiguo y el nuevo, respectivamente.

   Es importante considerar **cómo** para asignar bases de datos desde el dispositivo de hardware antiguo a las bases de datos del nuevo dispositivo de hardware.Usted hace el mapeo real de los dispositivos individuales mediante la selección de una cámara correspondiente, micrófono, entrada, salida o **Ninguno** en la columna de la derecha.

Importante: Asegúrese de asignar **todas las** cámaras, micrófonos, entradas, salidas, etc.Contenido asignan a **Ninguno**, se **perdieron**.



Ejemplo del dispositivo de hardware antiguo que tiene más dispositivos individuales que la nueva:



Haga clic en **Siguiente**.

6. Se le presentará una lista de hardware que se añaden, sustituyen o eliminados. Haga clic en **Confirmar**.

7. El paso final es un resumen de los dispositivos añadidos, sustituidos y heredadas y sus configuraciones. Haga clic en **Copiar en el portapapeles** copiar el contenido al portapapeles de Windows y / o **Cerrar** para cerrar el asistente.

Reemplazar un servidor de grabación

Si un servidor de grabación no está funcionando bien y desea sustituirlo por un nuevo servidor que hereda la configuración del servidor de grabación antigua:

1. Recuperar el ID del servidor de grabación desde el servidor de grabación antigua:
    1. Seleccionar **servidores de grabación**, a continuación, en el panel **general** seleccionar el servidor de grabación de edad.
    2. Seleccione la pestaña **almacenamiento**.
    3. Presione y mantenga presionada la tecla CTRL del teclado mientras selecciona la pestaña **Información**.
    4. Copie el número de ID del servidor de grabación en la parte inferior de la ficha **Info**.No copie el término ID, sólo el número en sí.

2. Vuelva a colocar el ID de servidor de grabación en el nuevo servidor de grabación:
    1. Detener el servicio de grabación de servidor en el servidor de grabación de edad, a continuación, en **Servicios** de Windows establezca **el tipo de inicio** del servicio a **deshabilitado**.

    Importante: Es muy importante que no se empieza dos servidores de grabación con ID idénticos al mismo tiempo.

    2. En el nuevo servidor de grabación, abra un explorador y vaya al C:\ProgramData\Milestone\XProtect Recording Server o la ruta donde se encuentra el servidor de grabación.
    3. Abra el archivo RecorderConfig.xml.
    4. Eliminar el ID indicado entre las etiquetas <id> y </ id> .

    5. Pegue el ID de servidor de grabación copiado entre las etiquetas <id> y
    6. /id>.Guarde el archivo RecorderConfig.xml.
    7. Ir al registro:HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\VideoOS\Recorder\Installation.
    8. Abra **RecorderIDOnMachine** y cambie el ID antiguo del servidor de grabación con el nuevo ID.
    9. Reinicie el servicio Servidor de grabación. Cuando el nuevo servicio Recording Server se pone en marcha, que ha heredado todos los ajustes del servidor de grabación de edad.

Controladores de dispositivo de vídeo (drivers)

Controladores de dispositivo (explicados)

Su sistema utiliza los controladores de dispositivos de video para controlar y comunicarse con los dispositivos de cámara conectada a un servidor de grabación. Debe instalar los controladores de dispositivo en cada servidor de grabación en su sistema.

A partir de la versión 2018 R1, los controladores del dispositivo se dividen en dos paquetes de dispositivos: el paquete de dispositivo regular con controladores más nuevos y un paquete de dispositivo heredado con controladores más antiguos.

El paquete de dispositivo regular se instala automáticamente cuando instala el servidor de grabación. Más tarde, puede actualizar los controladores descargando e instalando una versión más nueva del paquete de dispositivo. Milestone publica regularmente nuevas versiones de controladores de dispositivos y los pone a disposición en la página de descarga (http://www.milestonesys.com/downloads) en nuestro sitio web como paquetes de dispositivos. Cuando actualiza un paquete de dispositivo, puede instalar la última versión sobre cualquier versión que tenga instalada.

El paquete de dispositivo heredado solo se puede instalar si el sistema tiene un paquete de dispositivo normal instalado. Los controladores del paquete de dispositivo heredado se instalan automáticamente si ya hay una versión anterior instalada en su sistema. Está disponible para descarga e instalación manual en la página de descarga de software (http://www.milestonesys.com/downloads).

Detenga el servicio Recording Server antes de realizar la instalación; de lo contrario, deberá reiniciar la computadora.

Para garantizar el mejor rendimiento, siempre use la última versión de los controladores del dispositivo.

Acerca de la eliminación de los controladores de dispositivos de vídeo

Si ya no necesita controladores de dispositivo de vídeo en su ordenador, puede eliminar los paquetes de dispositivos de su sistema. Para ello, siga el procedimiento estándar de Windows para eliminar programas.

Si quita los controladores de dispositivos de vídeo, el servidor de grabación y los dispositivos de la cámara no se pueden comunicar por más tiempo. No quitar paquetes de dispositivos cuando se actualiza porque se puede instalar una nueva versión en la parte superior de una antigua. Sólo si desinstala todo el sistema, es posible retirar el paquete de dispositivos.

Servicios Managing server

En la computadora que ejecuta los servicios del servidor, encontrará los iconos de la bandeja del administrador del servidor en el área de notificación. A través de estos íconos, puede obtener información sobre los servicios y realizar ciertas tareas. Esto incluye, por ejemplo, comprobar el estado de los servicios, o ver los registros de los mensajes de estado, y iniciar y detener los servicios.

Iconos de la bandeja del administrador del servidor (explicados)

Los iconos de la bandeja en la tabla muestran los diferentes estados de los servicios que se ejecutan en el servidor de gestión, el servidor de grabación, el servidor de grabación de conmutación por error y el servidor de eventos. Son visibles en las computadoras con los servidores instalados, en el área de notificación:

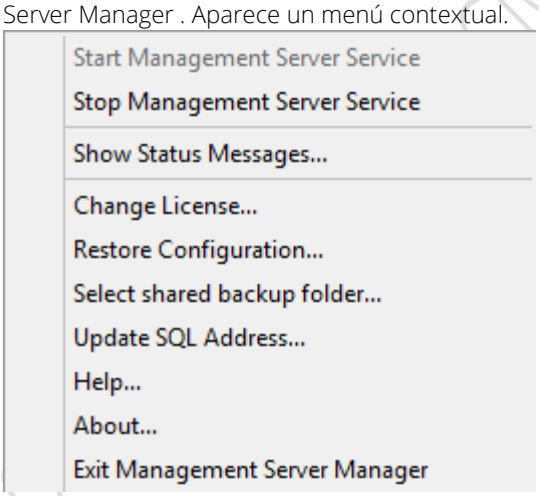
Icono de Management Server Manager	Icono de Recording Server Manager	Icono de Event Server Manager	Icono de Failover Recording Server Manager	Descripción
				**Ejecutando** Aparece cuando un servicio de servidor está activado y se inicia. Si el servicio Failover Recording Server se está ejecutando, se puede asumir el control si falla el servidor de grabación estándar.
				**Detenido** Aparece cuando un servicio de servidor se ha detenido. Si el servicio Failover Recording Server se detiene, no se puede asumir el control si falla el servidor de grabación estándar.
				**Comenzando** Aparece cuando un servicio de servidor se encuentra en el proceso de arranque. En circunstancias normales, el icono de la bandeja cambia después de un corto tiempo a **Ejecutando**.
				**Parada** Aparece cuando un servicio de servidor está en el proceso de detener. En circunstancias normales, el icono de bandeja cambia después de un corto tiempo para **Detenido**.
				**En estado indeterminado** Aparece cuando el servicio de servidor se carga inicialmente y hasta que se recibe la primera información, en la que el icono de la bandeja, en circunstancias normales, los cambios a partir **comenzando** y después para **Ejecutando**.
				**Correr fuera de línea** Aparece normalmente cuando el servicio Recording Server o Failover recording se está ejecutando, pero el servicio Management Server no lo es.

Icono de Management Server Manager	Icono de Recording Server Manager	Icono de Event Server Manager	Icono de Failover Recording Server Manager	Descripción
				**Debe ser autorizado por el administrador** Aparece cuando el servicio Recording Server se carga por primera vez. Los administradores autorizar el servidor de impresión a través del Management Client: Ampliar los **Servidores** lista, seleccione el nodo del **servidor de grabación** y en el panel general, haga clic en el servidor de registro pertinente y seleccione **Autorizar servidor de grabación**.

Iniciar o detener el servicio Management Server

El icono de la bandeja del Management Server Manager indica el estado del servicio Management Server, por ejemplo **Running/En ejecución**. A través de este icono, puede iniciar o detener el servicio Management Server. Si detiene el servicio Management Server, no puede usar el Management Client.

1. En el área de notificación, haga clic con el botón derecho en el ícono de la bandeja del Management Server Manager . Aparece un menú contextual.



2. Si el servicio se ha detenido, haga clic en **servicio Start Management Server** para iniciarlo. El icono de bandeja cambia para reflejar el nuevo estado.

3. Para detener el servicio, haga clic en **Detener servicio Management Server**.

Para obtener más información sobre los iconos de la bandeja, consulte Iconos de la bandeja del administrador del servidor (explicado) (ver "Iconos de la bandeja del administrador del servidor (explicados)" en la página 462).

Ver también

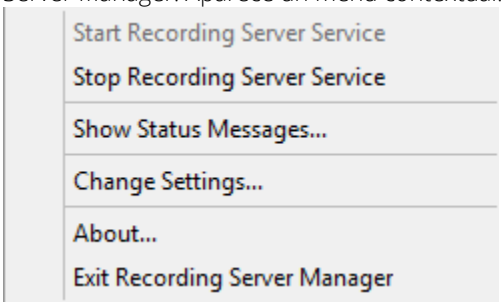
Iniciar, detener o reiniciar el servicio Event Server (en la página 466)

Iniciar o detener el servicio Recording Server (en la página 465)

Iniciar o detener el servicio Recording Server

El icono de la bandeja del Recording Server Manager indica el estado del servicio Servidor de grabación, por ejemplo **Running/En ejecución**. A través de este icono, puede iniciar o detener el servicio Recording Server. Si se detiene el servicio Recording Server, el sistema no puede interactuar con los dispositivos conectados al servidor. Esto significa que no puede ver el vídeo en directo o grabar vídeo.

1. En el área de notificación, haga clic con el botón derecho en el icono de la bandeja del Recording Server Manager. Aparece un menú contextual.



2. Si el servicio se ha detenido, haga clic en **servicio Start Recording Server** para iniciarlo. El icono de bandeja cambia para reflejar el nuevo estado.

3. Para detener el servicio, haga clic en **Detener servicio Recording Server**.

Para obtener más información sobre los iconos de la bandeja, consulte Los iconos de la bandeja (explicados) (ver "Iconos de la bandeja del administrador del servidor (explicados)" en la página 462).

Ver también

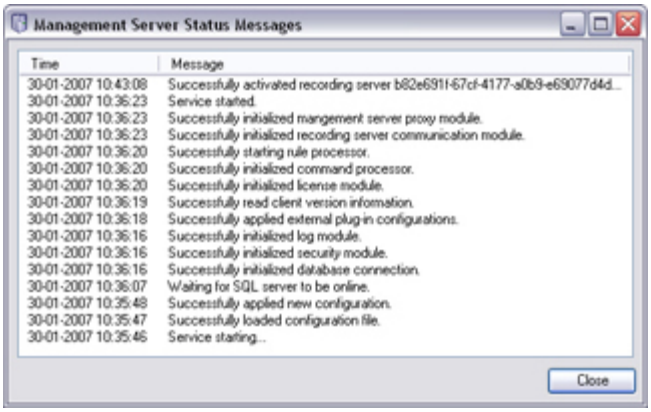
Iniciar, detener o reiniciar el servicio Event Server (en la página 466)

Iniciar o detener el servicio Management Server (en la página 464)

Ver mensajes de estado para el servidor de gestión o servidor de grabación

1. En el área de notificación, haga clic en el icono de la bandeja correspondiente. Aparece un menú contextual.

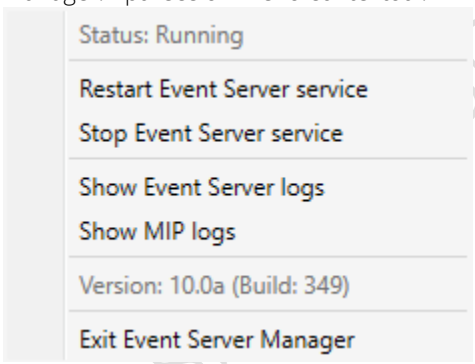
2. Seleccione **Mostrar mensajes de estado**.Dependiendo del tipo de servidor, aparece ya sea la ventana los **mensajes de estado de servidor de gestión** o **mensajes de estado del servidor de grabación** con una lista mensajes de estado con fecha y hora:



Iniciar, detener o reiniciar el servicio Event Server

El icono de la bandeja de Event Server Manager indica el estado del servicio del servidor de eventos, por ejemplo **Running/En ejecución**. A través de este icono, puede iniciar, detener o reiniciar el servicio Event Server. Si se detiene el servicio, partes del sistema no funcionarán, incluyendo eventos y alarmas. Sin embargo, todavía se puede ver y grabar vídeo. Para obtener más información, vea Detener el servicio Event Server.

1. En el área de notificación, haga clic con el botón derecho en el icono de la bandeja del Event Server Manager. Aparece un menú contextual.



2. Si el servicio se ha detenido, haga clic en **servicio Start Event Server** para iniciarlo. El icono de bandeja cambia para reflejar el nuevo estado.

3. Para reiniciar o detener el servicio, haga clic en **Reiniciar servicio Event Server** o **Detención de servicio Event Server**.

Para obtener más información sobre los iconos de la bandeja, consulte Iconos de la bandeja del administrador del servidor (explicado) (ver "Iconos de la bandeja del administrador del servidor (explicados)" en la página 462).

Ver también

Iniciar o detener el servicio Recording Server (en la página 465)

Detener el servicio Event Server (en la página 467)

Detener el servicio Event Server

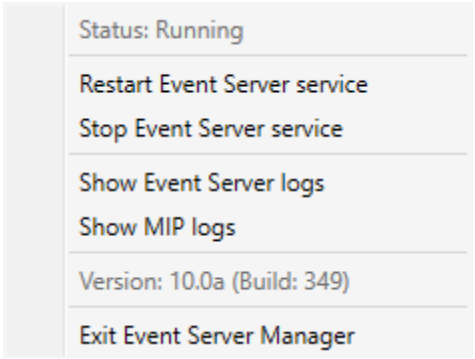
Al instalar MIP plug-ins en el servidor de eventos, primero debe detener el servicio Servidor de eventos y, a continuación, después, reiniciarlo. Sin embargo, mientras que el servicio se detiene, muchas áreas del sistema VMS no funcionarán:

- No hay eventos o alarmas se almacenan en el servidor de eventos. Sin embargo, sistemas y dispositivos eventos aún desencadenan acciones, por ejemplo, iniciar la grabación.
- XProtect Access, XProtect LPR y XProtect Transact no funcionan en la configuración o en XProtect Smart Client.
- Eventos analíticos no funcionan.
- Los eventos genéricos no funcionan.
- No hay alarmas se disparan.
- En XProtect Smart Client, mapa elementos de vista, lista de alarmas visualizar los objetos, y el espacio de trabajo Administrador de alarmas no funcionan.
- MIP plug-ins en el Servidor de eventos no se pueden ejecutar.
- Los complementos MIP en Management Client y XProtect Smart Client no funcionan correctamente.

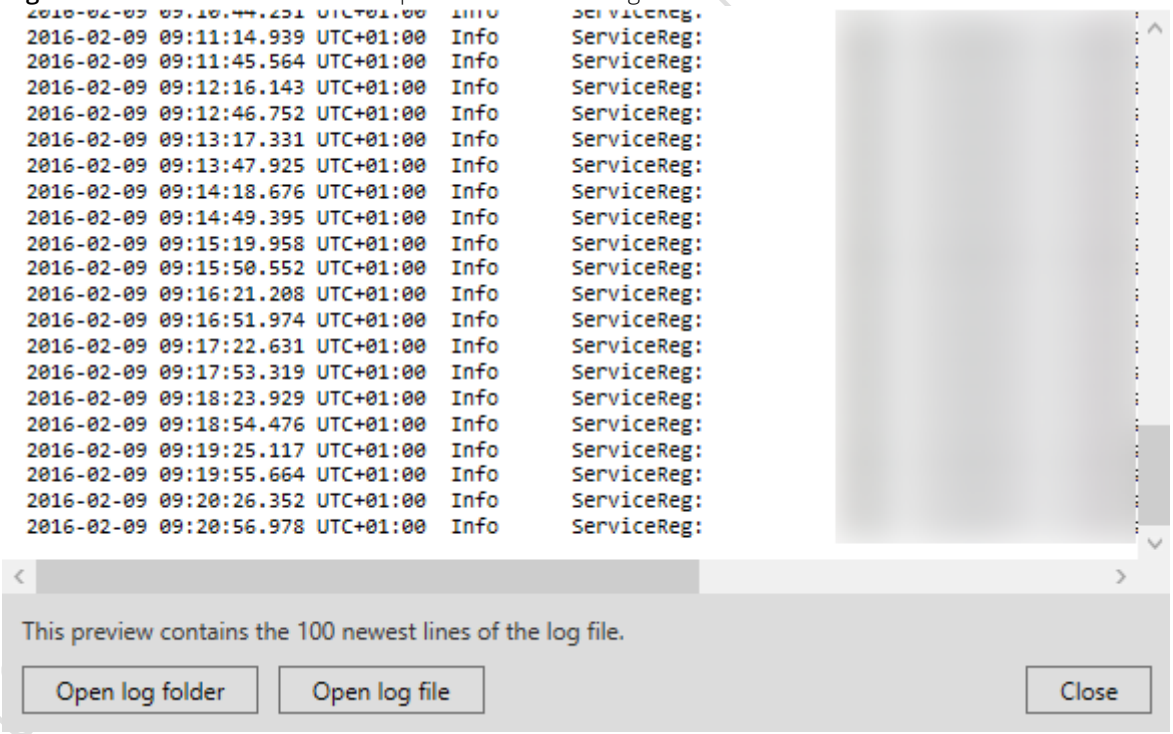
Ver Servidor de eventos o registros de MIP

Puede consultar la información de marca de tiempo sobre las actividades de eventos de servidores en el registro de eventos del servidor. Información sobre integraciones de terceros se registra en el registro de MIP en una subcarpeta en la carpeta del **servidor de eventos**.

1. En el área de notificación, haga clic en el icono de la bandeja correspondiente. Aparece un menú contextual.



2. Para ver las 100 líneas más recientes en el registro del servidor de sucesos, haga clic en **Mostrar registros del servidor de sucesos**.Aparece un visor de registro.



   1. Para ver el archivo de registro, haga clic en **Abrir archivo de registro**.
   2. Para abrir la carpeta de registro, haga clic en **Abrir carpeta de registro**.

3. Para ver las 100 líneas más recientes en el registro MIP, vuelva al menú contextual y haga clic en **Mostrar registros MIP**.Se muestra un visor de registro.

Si alguien elimina los archivos de registro del directorio de registro, los elementos de menú están atenuados. Para abrir el visor de registro, primero tiene que copiar los archivos de registro de nuevo en una de estas carpetas:C:\ProgramData\Milestone\XProtect Event Server\logs o C:\ProgramData\Milestone\XProtect Event Server\logs\MIPLogs.

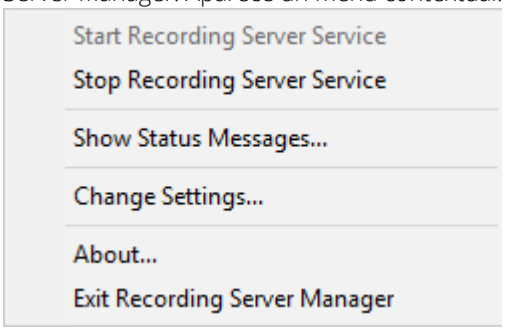
Cambiar la configuración del servicio del Recording Server

Puede cambiar los ajustes básicos para el servicio Recording Server, tales como los números de puerto a utilizar.

Requisitos
Debe detener el servicio Recording Server. Mientras que el servicio Recording Server se detiene, el sistema no puede interactuar con los dispositivos conectados al servidor de grabación. Esto significa que no puede ver el vídeo en directo o grabar vídeo.

Para cambiar la configuración:

1. En el área de notificación, haga clic con el botón derecho en el icono de la bandeja del Recording Server Manager. Aparece un menú contextual.



2. Seleccionar **servicio Stop Recording Server**.
3. Haga clic con el icono de la bandeja de nuevo.
4. Seleccione **Cambie la configuración**. Aparecerá la ventana de **configuración de los servidores de grabación**. Cambie los ajustes adecuados.

Ver también

Configuración del servidor de grabación (en la página 469)

Configuración del servidor de grabación

Al configurar Registrar los ajustes de servidor, especifique lo siguiente:

Nombre	Descripción
Dirección	Dirección IP (ejemplo:123. 123. 123. 123) o nombre de host (ejemplo: ourserver) del servidor de gestión a la que el servidor de registro deben estar conectados. Esta información es necesaria para que el servidor de grabación se puede comunicar con el servidor de gestión.
Puerto	Número de puerto que se utilizará cuando se comunica con el servidor de gestión. Predeterminado es el puerto 9993. Puede cambiarlo si es necesario.
Puerto del servidor Web	Número de puerto que se utilizará para el manejo de peticiones al servidor web, por ejemplo para el manejo de los comandos de control de cámaras PTZ y para la navegación de las solicitudes de los vivos y el XProtect Smart Client. Predeterminado es el puerto 7563. Puede esto si es necesario.

Nombre	Descripción
Alerta de puerto del servidor	Número de puerto que se utilizará cuando el servidor de grabación a la escucha de información de TCP (algunos dispositivos utilizan TCP para enviar mensajes de eventos). Predeterminado es el puerto 5432. Puede cambiarlo si es necesario.
Puerto del servidor SMTP	Número de puerto que se utilizará cuando el servidor de grabación de escucha para obtener información simple de transferencia de correo (SMTP). SMTP es un estándar para el envío de mensajes de correo electrónico entre servidores. Algunos dispositivos utilizan SMTP para enviar mensajes de eventos o imágenes al servidor del sistema de vigilancia a través del correo electrónico.El valor predeterminado es el puerto 25, que se puede activar y desactivar. Se puede cambiar el número de puerto si es necesario.

Reinicio servicio de Data Collector Server

El sistema instala automáticamente el servicio **Data Collector Server** en los mismos equipos que el servidor de administración, el servidor de grabación, el servidor de registro, el servidor de eventos y el servidor Milestone Mobile.

Normalmente, el servicioData Collector Server no requiere mantenimiento, pero si el servicio se **detiene**, no se envía ningún feed en vivo al Monitor de sistema.Esto se indica en el Monitor del sistema con mensajes de error.

1. En el equipo donde está instalado el servicio Data Collector Server:
2. En menú inicio **Windows**, seleccionar **Panel de control**, y luego:
   - Si se utiliza **Categoría** vista, encontrar el categoría **Sistema y Seguridad** y haga clic en **Herramientas administrativas**.
   - Si se utiliza **iconos pequeños** o **iconos grandes**, haga clic en **Herramientas administrativas**.
3. Haga doble clic en **Servicios**.
4. Busque el **Milestone XProtect Data Collector Server**.Haga clic en él y seleccione **Inicio** para reiniciar el servicio.

Servicios registrados

De vez en cuando, tiene servidores y / o servicios que deben ser capaces de comunicarse con el sistema, incluso si no son directamente parte del sistema. Algunos de los servicios, pero no todos, pueden registrarse automáticamente en el sistema. Los servicios que de forma automática se pueden registrar son:

- Servicio Event Server
- Log Server-tjänst
- Servicio Service Channel

Servicios registrados automáticamente se muestran en la lista de servicios registrados.

Puede especificar manualmente los servidores / servicios como servicios registrados del Management Client.

Canal de servicio (explicado)

El canal de servicio permite la comunicación configuración automática y transparente entre los servidores y clientes en su sistema. Por ejemplo, es el canal de servicio que se asegura de que cuando se cambia una visión compartida de un cliente, el cambio se refleja inmediatamente en otros clientes utilizando el punto de vista compartido relevante. El canal de servicio también facilita la comunicación relacionada con la configuración entre servidores y clientes en los casos en los que utilice varios plug-ins o los productos complementarios de con el sistema.

El canal de servicio normalmente se instala como parte de la instalación del servidor de gestión y reside en el equipo servidor de gestión, pero si es necesario, es posible que sólo así instalarlo en otro servidor en su sistema de vigilancia.

Una vez instalado, el canal de servicio puede registrar automáticamente con el sistema (es decir, que se convierte automáticamente en la lista de los servicios registrados característica en el Management Client). Su ubicación es conocida por el sistema, y los clientes conectarse al sistema que puede beneficiarse de ella automáticamente.

Si más tarde cambia la dirección IP o el nombre de host del servidor que ejecuta el servicio de canal de servicio, debe editar manualmente la información en **herramienta** > **Servicios registrados** en el Management Client. Además, si más adelante necesita cambiar el usuario con el que se ha instalado el servicio de canal de servicio, debe quitar el servicio Service Channel y después instalarlo de nuevo bajo el nuevo usuario.

Es importante que cualquier instancia de XProtect Smart Client es el tiempo sincronizado con el equipo que ejecuta el servicio Service Channel. Si el XProtect Smart Client no es el tiempo sincronizado con el servidor de gestión y el equipo que ejecuta el servicio Service Channel, el XProtect Smart Client no se actualiza con información sobre los cambios de configuración realizados por otros usuarios de XProtect Smart Client. Esto significa que el riesgo de los usuarios sobrescribir los cambios de configuración de cada uno. Si sus XProtect Smart Client no son de tiempo sincronizado con el equipo que ejecuta el servicio Service Channel, aparece un error informándole de ello.

Añadir y editar servicios registrados

1. En ventana **Añadir/borrar servicios registrados**, haga clic en **Añadir** o **Editar** , dependiendo de sus necesidades.
2. En ventana **Añadir el servicio registrado** o **Editar el servicio registrado** (dependiendo de su selección anterior), especificar o editar los valores.
3. **Haga clic en OK (aceptar)**.

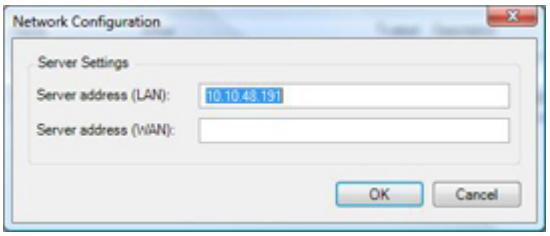
Administrar la configuración de red

Con los ajustes de configuración de red, puede especificar el servidor del servidor de gestión de redes LAN y WAN se dirige por lo que el servidor de gestión y los servidores de confianza pueden comunicarse.

1. En ventana **Añadir/borrar servicios registrados**, haga clic en **Red**.
2. Especificar la LAN y / o dirección IP WAN del servidor de gestión.

   Si todos los servidores implicados (tanto en el servidor de gestión y los servidores de confianza) están en su red local, sólo tiene que especificar la dirección LAN. Si uno o más servidores involucrados

acceden al sistema a través de una conexión a Internet, también debe especificar la dirección de la WAN.



3. **Haga clic en OK (aceptar)**.

Propiedades servicios registrados

En el **Añadir/borrar servidores registrados** o **Editar el servicio registrado** ventana, especifique lo siguiente:

Componente	Requisitos
Tipo	Campo precargada.
Nombre	Nombre del servicio registrado. El nombre se utiliza únicamente con fines de exhibición del Management Client.
URL	Haga clic en **Añadir** para agregar la dirección IP o el nombre de host del servicio registrado.Si se especifica un nombre de host como parte de una dirección URL, el anfitrión debe existir y estar disponible en la red. Las URL deben comenzar con http:// o https:// y no deben contener ninguno de los siguientes caracteres:< > & ' " * ? | [ ] ". **Ejemplo** de un formato de URL típico: http://ipaddress:port/directory (donde puerto y directorio son opcionales).Observe que puede añadir más de una dirección URL si es necesario.
De confianza	Seleccione si el servicio registrada debe ser de confianza inmediatamente (esto es a menudo el caso, pero la opción le da la flexibilidad para añadir el servicio registrada y luego marcarlo como de confianza mediante la edición de los servicios registrados más adelante). Tenga en cuenta que cambiar el estado de confianza también cambia el estado de otros servicios registrados compartir una o más de las direcciones URL definidas para el servicio registrada correspondiente.
Descripción	Descripción del servicio registrado. La descripción sólo se utiliza con fines de exhibición del Management Client.
Avanzados	Cuando un servicio es avanzado, tiene planes específicos de URI (por ejemplo, http, https, TCP o UDP) que necesitan ser establecido para cada dirección de host que defina. Por tanto, una dirección de host tiene varios puntos finales, cada uno con su propio esquema, dirección de host y el puerto IP de ese esquema.

Índice

D

E

F

G

H

I

L

M

Q

R

S

V

X

helpfeedback@milestone.dk

Acerca de Milestone Systems

Milestone Systems es un proveedor líder de software de gestión de vídeo de plataforma abierta, una tecnología que ayuda a determinar cómo garantizar la seguridad, proteger los activos y aumentar la eficiencia empresarial. Milestone Systems da soporte a una comunidad de plataforma abierta que fomenta la colaboración y la innovación en el desarrollo y uso de tecnologías de vídeo en red, con soluciones fiables y escalables que han probado su eficacia en más de 150 000 instalaciones en todo el mundo. Milestone Systems se fundó en 1998 y es una empresa independiente dentro del Grupo Canon.
Si desea más información, visite http://www.milestonesys.com.