MAKE THE
WORLD SEE

Milestone Systems

XProtect® VMS 2023 R2

Manual del administrador

XProtect Corporate
XProtect Expert
XProtect Professional+
XProtect Express+

milestone

Contenido

Copyright, marcas comerciales y exención de responsabilidad **26**

Generalidades **27**

Novedades 27

En Management Client 2023 R1 27

Iniciando sesión (explicación) 28

Autorización adicional (explicación) 29

Iniciar sesión utilizando una conexión no segura 30

Cambiar su contraseña de usuario básico 30

Descripción general del producto 31

Componentes del sistema 32

Servidor de gestión (explicación) 32

Instalaciones SQL Server y bases de datos (explicación) 33

Servidor de grabación (explicación) 33

Servidor móvil (explicación) 35

Servidor de eventos (explicación) 35

Servidor de registros (explicación) 35

API Gateway (explicación) 36

Failover 36

XProtect Management Server Failover 36

Servidor de gestión de failover (explicación) 37

Servidor de grabación de failover (explicación) 37

Funcionalidad del servidor de grabación de failover (explicación) 39

Pasos de failover (explicación) 41

Servicios de servidor de grabación de failover (explicación) 42

Clientes 43

Management Client (explicación) 43

XProtect Smart Client (explicación) 43

XProtect Mobile cliente (explicación) 44

XProtect Web Client (explicación) 45

Productos add-on 46

XProtect Access (explicación) ... 46
XProtect Incident Manager ... 47
XProtect LPR (explicación) ... 48
XProtect Smart Wall (explicación) ... 49
XProtect Transact (explicación) ... 50
Milestone Open Network Bridge (explicación) ... 50
XProtect DLNA Server (explicación) ... 51
Dispositivos ... 51
Hardware (explicación) ... 51
Preconfiguración de hardware (explicación) ... 52
Devices (explicación) ... 53
Cámaras ... 53
Micrófonos ... 53
Altavoces ... 54
Metadatos ... 54
Entradas ... 54
Salidas ... 54
Device groups (explicación) ... 55
Almacenamiento multimedia ... 56
Almacenamiento y archivado (explicación) ... 56
Estructura del archivo (explicación) ... 61
Almacenamiento previo en búfer y almacenamiento de grabaciones (explicación) ... 63
Almacenamiento de las grabaciones temporales del búfer previo ... 63
Autenticación ... 63
Active Directory (explicación) ... 63
Usuarios (explicación) ... 64
Usuarios de Windows ... 64
Usuarios básicos ... 65
Identity Provider (explicación) ... 65
IDP externo (explicación) ... 65
Reclamaciones (explicación) ... 65
Habilitar a los usuarios para iniciar sesión en el VMS de XProtect desde un IDP externo ... 66

Redirigir URI ... 66
Nombres de usuario únicos para usuarios de IDP externos ... 66
Ejemplo de reclamaciones de un IDP externo ... 66
Utilizar el número de secuencia de la demanda para crear nombres de usuario en XProtect ... 67
Definir reclamaciones específicas para crear nombres de usuario en XProtect ... 68
Eliminación de usuarios de IDP externos ... 68
Seguridad ... 69
Cometidos y permisos de un cometidos (explicación) ... 69
Permisos de un cometido ... 70
Máscara de privacidad (explicación) ... 71
Máscara de privacidad (explicación) ... 71
Perfiles Management Client (explicación) ... 73
Smart Client perfiles (explicación) ... 74
Bloqueos de evidencias (explicación) ... 75
Reglas y eventos ... 77
Reglas (explicación) ... 77
Complejidad de las reglas ... 78
Reglas y eventos (explicación) ... 79
Perfiles temporales (explicación) ... 81
Perfiles temporales de duración de día (explicación) ... 82
Perfiles de notificación (explicación) ... 82
Requisitos para crear perfiles de notificación ... 82
Eventos definidos por el usuario (explicación) ... 83
Eventos de análisis (explicación) ... 84
Eventos genéricos (explicación) ... 85
Webhooks (explicado) ... 85
Alarmas ... 86
Alarmas (explicación) ... 86
Configuración de alarma ... 87
Plano inteligente ... 88
Plano inteligente (explicación) ... 88
Integración de planos inteligentes con Google Maps (explicación) ... 89

Añadir firma digital a la clave Maps Static API ... 90
Integración de planos inteligentes con Bing Maps (explicación) ... 90
Archivos de planos inteligentes en caché (explicación) ... 90
Arquitectura ... 91
Una configuración de sistema distribuida ... 91
Milestone Interconnect (explicación) ... 92
Seleccionar Milestone Interconnect o Milestone Federated Architecture (explicación) ... 93
Milestone Interconnect y licencia ... 94
Milestone Interconnect ajustes (explicación) ... 94
Configuración de Milestone Federated Architecture ... 95
Puertos utilizados por el sistema ... 99
Grupos de aplicaciones ... 115
Grupos de aplicaciones en Milestone XProtect ... 115
Trabajar con grupos de aplicaciones ... 116
Abra la página Grupos de aplicaciones ... 116
Comparación de productos ... 116
Licencias ... 117
Licencias (explicación) ... 117
Gratis XProtect Essential+ ... 117
Licencias para productos VMS XProtect (excepto XProtect Essential+) ... 117
Tipos de licencia ... 118
Licencias básicas ... 118
Licencias de dispositivo ... 118
Licencias de cámara para Milestone Interconnect™ ... 119
Licencias de productos add-on ... 119
Activación de licencia (explicación) ... 119
Activación de licencia automática (explicación) ... 119
Periodo de gracia para la activación de la licencia (explicación) ... 120
Cambios en el dispositivo sin activación (explicación) ... 120
Cálculo del número disponible de cambios de dispositivo sin activación (explicación) ... 121
Milestone Care™ (explicación) ... 122
Licencias y sustitución de hardware (explicación) ... 123

Obtener una visión general de sus licencias ... 123
Activar sus licencias ... 124
Activar la activación automática de licencia ... 124
Deshabilitar la activación automática de licencia ... 125
Activar licencias en línea ... 125
Activar licencias fuera de línea ... 125
Activar licencias después del periodo de gracia ... 126
Obtener licencias adicionales ... 126
Cambiar el código de licencia del software ... 127
Desde el icono de la bandeja del servidor de gestión ... 127
Desde Management Client ... 127
Ventana de información de la licencia ... 128
Requisitos y consideraciones ... 132
Horario de verano (explicación) ... 132
Servidores de tiempo (explicación) ... 132
Limitar el tamaño de la base de datos ... 133
IPv6 y IPv4 (explicación) ... 133
Escribir direcciones IPv6 (explicación) ... 135
Uso de las direcciones IPv6 en las URL ... 135
Servidores virtuales ... 136
Múltiples servidores de gestión (clustering) (explicación) ... 136
Requisitos para el clustering ... 137
Proteger las bases de datos de grabación de la corrupción ... 137
Fallo del disco duro: proteger las unidades ... 137
Gestor de tareas de Windows: tenga cuidado al finalizar los procesos ... 138
Cortes de energía: usar un SAI ... 138
Registro de transacciones de la base de datos SQL (explicación) ... 138
Requisitos mínimos del sistema ... 139
Antes de comenzar la instalación ... 139
Preparar sus servidores y red ... 139
Preparar Active Directory ... 140
Método de instalación ... 140

Decidir sobre una edición de SQL Server ... 143
Seleccione cuenta de servicio ... 144
Autenticación Kerberos (explicación) ... 144
Exclusiones del escaneo de virus (explicación) ... 146
¿Cómo se puede configurar XProtect VMS para que funcione en modo compatible con FIPS 140-2? ... 148
Antes de instalar XProtect VMS en un sistema habilitado para FIPS ... 148
Registrar el código de licencia de software ... 148
Controladores de dispositivos (explicación) ... 149
Requisitos para la instalación fuera de línea ... 149
Comunicación segura (explicación) ... 150
Instalación ... 151
Instalar un nuevo sistema XProtect ... 151
Instalar XProtect Essential+ ... 151
Instalar el sistema: opción de Equipo único ... 157
Instale su sistema: opción personalizada ... 163
Instalar nuevos componentes XProtect ... 170
Instalación a través de Download Manager (explicación) ... 170
Instale un Management Client a través de Download Manager ... 171
Instalar un servidor de grabación a través de Download Manager ... 171
Instalar un servidor de grabación de failover a través de Download Manager ... 175
Instalación de XProtect VMS utilizando puertos no predeterminados ... 177
Instalación silenciosa a través de una consola de línea de comandos (explicación) ... 177
Instalar un servidor de grabación de forma silenciosa ... 179
Instalar XProtect Smart Client en silencio ... 180
Instalar un servidor de registros de forma silenciosa ... 182
Instalación para grupos de trabajo ... 183
Instalar en un clúster ... 183
Utilizar un certificado para un IDP externo en un entorno de clúster ... 186
Solución de errores cuando una configuración de IDP externo está protegida con un certificado ... 187
Download Manager/página web de descarga ... 188
Download Managerde la configuración por defecto ... 190
Download Managerde los instaladores estándar (usuario) ... 192

Añadir/publicar componentes del instalador de Download Manager ... 192
Ocultar/eliminar componentes del instalador Download Manager ... 193
Instalador de paquete de dispositivos: debe descargarse ... 194
Archivos de registro de la instalación y solución de problemas ... 195
Configuración ... 196
Lista de tareas de configuración inicial ... 196
Servidores de grabación ... 198
Cambiar o verificar la configuración básica de un servidor de grabación ... 198
Registrar un servidor de grabación ... 199
Ver el estado del cifrado a los clientes ... 200
Especificar el comportamiento cuando el almacenamiento de la grabación no está disponible ... 201
Añadir un nuevo almacenamiento ... 202
Crear un archivo dentro de un almacenamiento ... 203
Adjuntar un dispositivo o grupo de dispositivos a un almacenamiento ... 203
Dispositivos deshabilitados ... 203
Editar los ajustes de un almacenamiento o archivo seleccionado ... 204
Habilitar la firma digital para la exportación ... 204
Cifrar sus grabaciones ... 205
Hacer una copia de seguridad de las grabaciones archivadas ... 207
Eliminar un archivo de un almacenamiento ... 208
Eliminar un almacenamiento ... 208
Mover grabaciones no archivadas de un almacenamiento a otro ... 209
Asignar servidores de grabación failover ... 209
Habilitar la multidifusión para el servidor de grabación ... 210
Habilitar la multidifusión para cámaras individuales ... 211
Definir la dirección pública y el puerto ... 212
Asignar rangos de IP locales ... 213
Filtrar el árbol de dispositivos ... 213
Filtrar el árbol de dispositivos ... 213
Características de los criterios de filtrado ... 213
Especificación de múltiples criterios de filtrado ... 213
Restablecimiento del filtro ... 214

Dispositivos deshabilitados 214
Servidores failover 214
Configurar y habilitar servidores de grabación por failover 214
Servidores de grabación de failover en grupo para la espera en frío 215
Ver el estado de cifrado en un servidor de grabación de failover 215
Ver mensajes de estado 217
Ver información de la versión 217
Hardware 217
Añadir hardware 217
Añadir hardware (diálogo) 218
Deshabilitar / habilitar el hardware 219
Editar hardware 219
Editar hardware (diálogo) 220
Habilitar/deshabilitar dispositivos individuales 223
Configurar una conexión segura con el hardware 224
Habilitar la PTZ en un codificador de vídeo 224
Cambiar contraseñas en dispositivos de hardware 225
Actualizar el firmware de los dispositivos de hardware 227
Añadir y configurar un IDP externo 229
Detalles de interfaz de usuario 229
Añadir un grupo de dispositivos 229
Especificar qué dispositivos incluir en un grupo de dispositivos 229
Dispositivos deshabilitados 230
Especificar propiedades comunes para todos los dispositivos de un grupo de dispositivos 230
Dispositivos deshabilitados 231
Habilitar/deshabilitar dispositivos mediante grupos de dispositivos 231
Dispositivos - Ajustes de cámara 232
Ver o editar ajustes de la cámara 232
Previsualizar 232
Rendimiento 232
Añadiendo hardware 232
Habilitar y deshabilitar la compatibilidad con lentes de ojo de pez 233

Especificar los ajustes de la lente ojo de pez ... 233
Dispositivos - Grabación ... 233
Habilitar/deshabilitar la grabación ... 233
Habilitar la grabación en los dispositivos relacionados ... 233
Gestionar la grabación manual ... 234
Añadir a cometidos: ... 234
Uso en reglas: ... 234
Especificar velocidad de grabación de fotogramas ... 234
Habilitar la grabación de fotogramas clave ... 235
Habilitar la grabación en los dispositivos relacionados ... 235
Guardar y recuperar grabación remota ... 236
Borrar grabaciones ... 236
Dispositivos - Ajustes de cámara ... 237
Transmisión adaptable (explicación) ... 237
Reproducción adaptativa (explicado) ... 237
Disponibilidad ... 237
Activar streaming adaptable ... 238
Grabaciones en Edge ... 238
Resolución del vídeo reproducido ... 238
Añadir un flujo ... 238
Gestionar la transmisión múltiple ... 239
Para cambiar el flujo que se utilizará para la grabación ... 239
Limitar la transmisión de datos ... 240
Ejemplos ... 240
Dispositivos - Almacenamiento ... 241
Gestionar almacenamiento previo en búfer ... 241
Habilitar y deshabilitar almacenamiento previo en búfer ... 241
Especificar el lugar de almacenamiento y el periodo de pre-búfer ... 241
Usar el pre-buffer en las reglas ... 242
Monitorizar el estado de las bases de datos para dispositivos ... 242
Mover dispositivos de un almacenamiento a otro ... 244
Dispositivos - Detección de movimiento ... 244

Detección de movimiento (explicación) 244
Calidad de imagen 245
Máscaras de privacidad 245
Habilitar y deshabilitar la detección de movimiento 245
Especificar la configuración por defecto de detección de movimiento para cámaras 245
Habilitar o deshabilitar la detección de movimiento para una cámara específica 245
Habilitar o deshabilitar la aceleración por hardware 246
Para habilitar o deshabilitar la aceleración por hardware 246
Uso de recursos de la GPU 246
Equilibrio de carga y rendimiento 246
Habilitar la sensibilidad manual para definir el movimiento 247
Especificar umbral para definir movimiento 248
Especificar regiones de exclusión para detección de movimiento 248
Dispositivos - Posiciones de cámara preestablecidas 249
La posición prestablecida inicial 249
Añadir una posición preestablecida (tipo 1) 249
Utilizar posiciones predefinidas desde la cámara (tipo 2) 252
Asignar la posición prestablecida de una cámara como predeterminada 252
Especificar el valor prestablecido predeterminado como la posición de inicio de PTZ 253
Habilitar configuración de la posición de inicio de PTZ 253
Editar una posición preestablecida para una cámara (solo tipo 1) 253
Cambiar el nombre de una posición predefinida para una cámara (solo tipo 2) 255
Probar una posición predefinida (solo tipo 1) 256
Dispositivos - Patrulla 256
Perfiles de patrulla y Patrulla manual (explicación) 256
Patrulla manual 256
Añadir un perfil de patrulla 257
Especificar posiciones predefinidas en un perfil de vigilancia 257
Especificar el tiempo en cada posición predefinida 258
Personalizar transiciones (PTZ) 258
Especificar una posición final al realizar la vigilancia 259
Reservar y liberar sesiones de PTZ 260

Reservar una sesión de PTZ ... 260
Liberar una sesión PTZ ... 261
Especificar tiempos de espera para sesiones de PTZ ... 261
Dispositivos - Eventos para reglas ... 262
Añadir o eliminar un evento para un dispositivo ... 262
Añadir un evento ... 262
Eliminar un evento ... 262
Especificar las propiedades del evento ... 262
Usar varias instancias de un evento ... 262
Dispositivos - Eventos para reglas ... 263
Habilitar/deshabilitar la máscara de privacidad ... 263
Definir las máscaras de privacidad ... 263
Cambiar el tiempo de espera de las máscaras de privacidad levantadas ... 265
Dar permiso a los usuarios para levantar las máscaras de privacidad ... 266
Crear un informe de su configuración de máscara de privacidad ... 267
Clientes ... 268
Grupos de vistas (explicación) ... 268
Añadir un grupo de vistas ... 269
Perfiles Smart Client ... 270
Añadir y configurar un perfil Smart Client ... 270
Copiar un perfil Smart Client ... 270
Crear y configurar perfiles, cometidos y perfiles temporales Smart Client ... 270
Establecer el número de cámaras permitidas durante la búsqueda ... 271
Cambiar los ajustes de exportación por defecto ... 275
Perfiles Management Client ... 276
Añadir y configurar un perfil Management Client ... 276
Copiar un perfil Management Client ... 277
Gestionar la visibilidad de la funcionalidad de un perfil de Management Client ... 277
Asociar un perfil de Management Client con un cometido ... 277
Gestionar el acceso general a la funcionalidad del sistema para un cometido ... 277
Limitar la visibilidad de la funcionalidad de un perfil ... 278
Matrix ... 278

Matrix y Matrix destinatarios (explicación) 278
Definir reglas que envían vídeo a destinatarios de Matrix 279
Añadir destinatarios de Matrix 279
Enviar el mismo vídeo a varias vistas de XProtect Smart Client 280
Reglas y eventos 280
Añadir reglas 280
Eventos 280
Acciones y acciones de parada 280
Crear una regla 281
Validar reglas 282
Validar una regla 283
Validar todas las reglas 283
Editar, copiar y cambiar el nombre de una regla 283
Desactivar y activar una regla 284
Especificar un perfil temporal 284
Añadir una sola hora 285
Añadir una hora recurrente 285
Tiempo recurrente 286
Editar un perfil temporal 286
Crear perfiles temporales de duración de día 287
Propiedades del perfil temporal de duración de día 287
Añadir perfiles de notificación 288
Desencadenar notificaciones de correo electrónico a partir de reglas 290
Añadir un evento definido por el usuario 290
Cambiar nombre de un evento definido por el usuario 291
Añadir y editar un evento de análisis 291
Añadir un evento de análisis 291
Editar un evento de análisis 292
Editar ajustes de eventos de análisis 292
Probar un evento de análisis 292
Añadir un evento genérico 293
Para añadir un evento genérico: 293

Autenticación ... 293
Registrar las reclamaciones de un PDI externo ... 293
Asignar reclamaciones de un IDP externo a cometidos en XProtect ... 294
Inicio de sesión a través de un IDP externo: ... 294
Seguridad ... 295
Añadir y gestionar un rol ... 295
Copiar, cambiar nombre o eliminar un rol ... 295
Copiar un rol ... 295
Cambiar nombre de un rol ... 295
Eliminar un rol ... 296
Ver roles efectivos ... 296
Asignar/eliminar usuarios y grupos a/de roles ... 296
Asignar usuarios de Windows y grupos a un rol ... 296
Asignar usuarios básicos a un rol ... 297
Quitar usuarios y grupos de un rol ... 297
Crear usuarios básicos ... 297
Configurar los ajustes de inicio de sesión para usuarios básicos ... 298
Para crear un usuario básico en su sistema: ... 299
Ver el estado del cifrado a los clientes ... 299
Panel del sistema ... 300
Ver tareas en curso actualmente en servidores de grabación ... 300
Monitor del sistema (explicación) ... 301
Panel de control del monitor del sistema (explicación) ... 301
Umbrales del monitor del sistema (explicación) ... 301
Ver el estado actual de su hardware y solucionar problema en caso necesario ... 302
Ver el estado histórico de su hardware e imprimir un informe ... 303
Recopilar datos históricos de los estados del hardware ... 303
Añadir un nuevo mosaico de servidores o cámaras al panel de control del monitor del sistema ... 304
Editar un mosaico de cámaras o servidores en el panel de control del monitor del sistema ... 304
Eliminar un mosaico de cámaras o servidores en el panel de control del monitor del sistema ... 305
Editar umbrales para cuando los estados del hardware deben cambiar ... 305
Ver bloqueos de evidencias en el sistema ... 306

Imprimir un informe con la configuración del sistema ... 307
Metadatos ... 307
Mostrar u ocultar categorías de búsqueda de metadatos y filtros de búsqueda ... 307
Alarmas ... 308
Añadir una alarma ... 308
Habilitar cifrado ... 309
Habilitar encriptación en y desde el servidor de gestión ... 309
Habilitar encriptación del servidor para servidores de grabación o servidores remotos ... 311
Habilitar el cifrado del servidor de eventos ... 313
Habilitar encriptación en clientes y servidores ... 315
Habilitar encriptación en el servidor móvil ... 316
Milestone Federated Architecture ... 318
Configurar su sistema para ejecutar sitios federados ... 318
Añadir sitio a la jerarquía ... 320
Aceptar la inclusión en la jerarquía ... 321
Establecer propiedades del sitio ... 321
Actualizar jerarquía del sitio ... 322
Iniciar sesión en otros sitios de la jerarquía ... 323
Actualizar la información de sitios secundarios ... 323
Separar un sitio de la jerarquía ... 323
Milestone Interconnect ... 324
Añadir un sitio remoto a su sitio central Milestone Interconnect ... 324
Asignar permisos de usuario ... 325
Actualizar el hardware del sitio remoto ... 325
Habilitar la reproducción directamente desde la cámara del sitio remoto ... 325
Recuperar grabaciones a distancia de la cámara del sitio remoto ... 326
Configurar el sitio central para que responda a los eventos de los sitios remotos ... 327
Servicios de conexión remota ... 328
Servicios de conexión remota (explicación) ... 328
Instalar un entorno de servidor de túnel seguro para la conexión de la cámara con un solo clic ... 329
Añadir o editar servidores de túneles seguros ... 329
Registrar una nueva cámara Axis One-Click ... 330

Planos inteligente ... 330
Entornos geográficos (explicación) ... 330
Habilitar Bing Maps o Google Maps en Management Client ... 331
Habilitar Bing Maps o Google Maps en XProtect Smart Client ... 332
Habilitar Milestone Map Service ... 332
Especificar servidor de fichas OpenStreetMap ... 333
Habilitar la edición de planos inteligentes ... 334
Habilitar la edición de dispositivos en el plano inteligente ... 335
Defina la posición del dispositivo y la dirección de la cámara, el campo de visión y la profundidad (plano inteligente) ... 336
Configurar el plano inteligente con Milestone Federated Architecture ... 338
Mantenimiento ... **340**
Hacer una copia de seguridad y restaurar la configuración del sistema ... 340
Hacer una copia de seguridad y restaurar la configuración del sistema (explicación) ... 340
Seleccionar la carpeta de copia de seguridad compartida ... 341
Hacer una copia de seguridad manual de la configuración del sistema ... 341
Restaurar la configuración del sistema a partir de una copia de seguridad manual ... 341
Contraseña de configuración del sistema (explicación) ... 343
Ajustes de la contraseña de configuración del sistema ... 343
Cambiar los ajustes de contraseña de la configuración del sistema ... 344
Introducir los ajustes de la contraseña de configuración del sistema (recuperación) ... 345
Manually backing up your system configuration (explicación) ... 346
Hacer una copia de seguridad y restaurar la configuración del servidor de eventos (explicación) ... 346
Copia de seguridad y restauración programada de la configuración del sistema (explicación) ... 346
Hacer una copia de seguridad de la configuración del sistema con una copia de seguridad programada ... 347
Restaurar la configuración del sistema a partir de una copia de seguridad programada ... 347
Copia de seguridad de la base de datos SQL del servidor de registro ... 348
Escenarios de fallos y problemas de copia de seguridad y restauración (explicación) ... 349
Mover el servidor de gestión ... 349
Unavailable management servers (explicación) ... 350
Mover la configuración del sistema ... 351
Sustituir un servidor de grabación ... 351
Mover el hardware ... 352

Mover el hardware (asistente) ... 353
Sustituir el hardware ... 356
Actualizar los datos de su hardware ... 359
Gestionar el SQL Server y la base de datos ... 360
Cambiar el SQL Server y las direcciones de la base de datos (explicación) ... 360
Cambiar el servidor de registro de SQL Server y la base de datos ... 360
Cambie el servidor de gestión y el servidor de eventos SQL Server y la base de datos. ... 361
Cambie el servidor de registro de XProtect Incident Manager SQL Server y la base de datos ... 361
Cambiar el servidor de Identity Provider de SQL Server y la base de datos ... 361
Gestión de los servicios del servidor ... 362
Iconos de la bandeja del administrador del servidor (explicación) ... 362
Iniciar o detener el servicio Management Server ... 365
Iniciar o detener el servicio Recording Server ... 365
Ver los mensajes de estado del Servidor de gestión o del Servidor de grabación ... 366
Gestionar el cifrado con el Server Configurator ... 366
Iniciar, detener o reiniciar el servicio Event Server ... 366
Detener el servicio Event Server ... 367
Ver Servidor de eventos o MIP registros ... 368
Introduzca la contraseña actual de configuración del sistema ... 369
Gestión de los servicios registrados ... 370
Añadir y editar servicios registrados ... 370
Gestionar la configuración de la red ... 371
Propiedades de los servicios registrados ... 371
Eliminación de los drivers de dispositivos (explicación) ... 372
Eliminar un servidor de grabación ... 372
Eliminar todo el hardware de un servidor de grabación ... 373
Cambiar el nombre de host del ordenador del servidor de gestión ... 373
La validez de los certificados ... 373
Pérdida de las propiedades de los datos de los clientes para los servicios registrados ... 374
En Milestone Customer Dashboard, el nombre del host aparecerá sin cambios ... 374
Un cambio de nombre de host puede provocar el cambio de la dirección SQL Server ... 374
Cambios de nombre de host en un Milestone Federated Architecture ... 375

El host del sitio es el nodo raíz de la arquitectura ... 375
El host del sitio es un nodo hijo en la arquitectura ... 375
Registros del servidor de gestión ... 376
Identificar actividad del usuario, eventos, acciones y errores ... 376
Filtrar registros ... 377
Exportar registros ... 378
Registros de búsqueda ... 379
Cambiar idioma del registro ... 379
Permita que 2018 R2 y los componentes anteriores escriban registros ... 380
Solución de problemas ... 381
Registros de depuración (explicación) ... 381
Emitir: El cambio de direcciones de bases de datos y SQL Server previene el acceso a las bases de datos ... 381
Emitir: El inicio del servidor de grabaciones falla debido a un conflicto de puertos ... 382
Emitir: Recording Server pasa a estar fuera de línea al cambiar al nodo del clúster de Management Server ... 383
Emitir: Un nodo principal en una configuración de Milestone Federated Architecture no puede conectar con un nodo secundario ... 384
Para restablecer la conexión entre el nodo principal y el sitio ... 384
Actualizar ... 385
Actualizar (explicación) ... 385
Requisitos de actualización ... 386
Actualizar XProtect VMS para ejecutar en modo compatible con FIPS 140-2 ... 387
Actualizar prácticas recomendadas ... 389
Actualizar en un clúster ... 391
Detalles de interfaz de usuario ... 392
Ventana y paneles principales ... 392
Diseño de paneles ... 394
Ajustes del sistema (cuadro de diálogo Opciones) ... 396
Pestaña General (opciones) ... 397
Pestaña Registros del servidor (opciones) ... 400
Pestaña Servidor de correo (opciones) ... 401
Pestaña Generación de AVI (opciones) ... 402
Pestaña Red (opciones) ... 403

Pestaña Marcador (opciones) 404
Pestaña Ajustes de usuario (opciones) 404
Pestaña IDP externo (opciones) 404
Configurar un IDP externo 405
Registrar reclamaciones 407
Añadir URI de redireccionamiento para los clientes web 408
Pestaña Panel de control del cliente (opciones) 408
Pestaña Bloqueo de evidencias (opciones) 408
Pestaña Mensajes de audio (opciones) 409
Pestaña Ajustes de privacidad 410
Pestaña Ajustes de control de acceso (opciones) 410
Pestaña Eventos de análisis (opciones) 411
Pestaña Alarmas y eventos (opciones) 412
Pestaña Eventos genéricos (opciones) 414
Menús de componentes 416
Management Client menús 416
Menú Archivo 416
Editar menú 416
Menú Ver 416
Menú Acción 417
Menú de herramientas 417
Menú Ayuda 418
Server Configurator (Utilidad) 418
Propiedades de la pestaña Encriptación 418
Servidores de registro 419
Selección de idioma 420
Estado del icono de la bandeja 421
Inicio y parada de servicios desde iconos de la bandeja 423
Management Server Manager (icono de bandeja) 423
Nodo básico 425
Información de licencias (nodo Aspectos básicos) 425
Información del sitio (nodo Aspectos básicos) 425

Nodo de servicios de conexión remota ... 426
Conexión de cámara Axis One-click (nodo Servicios de conexión remota) ... 426
Nodo de servidores ... 427
Servidores (nodo) ... 427
Servidores de grabación (nodo Servidores) ... 427
Ventana Ajustes del servidor de grabaciones ... 428
Propiedades de servidores de grabación ... 429
Pestaña Almacenamiento (servidor de grabación) ... 431
Pestaña Failover (servidor de grabación) ... 436
Pestaña Multidifusión (servidor de grabación) ... 438
Pestaña Red (servidor de grabación) ... 441
Servidores de failover (nodo Servidores) ... 441
Propiedades de la pestaña Información (servidor de failover) ... 443
Pestaña multidifusión (servidor de failover) ... 445
Propiedades de la pestaña Información (grupo de failover) ... 446
Propiedades de la pestaña Secuencia (grupo de failover) ... 447
Servidor remoto para Milestone Interconnect ... 447
Pestaña Información (servidor remoto) ... 447
Pestaña Ajustes (servidor remoto) ... 448
Pestaña Eventos (servidor remoto) ... 448
Pestaña Recuperación remota ... 448
Nodo de dispositivos ... 449
Dispositivos (nodo Dispositivos) ... 449
Iconos de estado de dispositivos ... 450
Cámaras (nodo Dispositivos) ... 453
Micrófonos (nodo DIspositivos) ... 453
Altavoces (nodo Dispositivos) ... 454
Metadatos (nodo Dispositivos) ... 454
Entrada (nodo Dispositivos) ... 454
Salida (nodo Dispositivos) ... 455
Pestañas de Dispositivos ... 456
Pestaña información (dispositivos) ... 456

Propiedades de la pestaña Información ... 456
Pestaña Ajustes (dispositivos) ... 458
Pestaña Flujos (dispositivos) ... 459
Tareas en la pestaña Flujos ... 460
Pestaña Grabar (dispositivos) ... 460
Tareas en la pestaña Grabar ... 462
Pestaña Movimiento (dispositivos) ... 462
Tareas en la pestaña Movimiento ... 463
Pestaña Valores preestablecidos (dispositivos) ... 465
Tareas en la pestaña Valores preestablecidos ... 467
Propiedades de la sesión de PTZ ... 468
Pestaña Vigilancia (dispositivos) ... 470
Tareas en la pestaña Vigilancia ... 472
Propiedades de vigilancia manual ... 472
Pestaña Objetivo ojo de pez (dispositivos) ... 473
Tarea en la pestaña Objetivo ojo de pez ... 474
Pestaña Eventos (dispositivos) ... 474
Tareas en la pestaña Eventos ... 474
Pestaña Evento (propiedades) ... 475
Pestaña Cliente (dispositivos) ... 475
Propiedades de la pestaña Cliente ... 476
Pestaña Enmascaramiento de la privacidad (dispositivos) ... 478
Tareas en la pestaña Enmascaramiento de la privacidad ... 479
Tareas relacionadas con el Enmascaramiento de la privacidad ... 479
Pestaña Enmascaramiento de la privacidad (propiedades) ... 480
Ventana de propiedades de hardware ... 481
Pestaña Información (hardware) ... 481
Pestaña Ajustes (hardware) ... 483
Pestaña PTZ (codificadores de vídeo) ... 483
Nodo cliente ... 484
Clientes (nodo) ... 484
Smart Wall (nodo Cliente) ... 484

Smart Wall propiedades ... 484
Propiedades del monitor ... 486
Smart Client Perfiles (nodo Cliente) ... 488
Pestaña Información (perfiles de Smart Client) ... 488
Pestaña General (perfiles de Smart Client) ... 489
Pestaña Avanzados (perfiles de Smart Client) ... 489
Pestaña Directo (perfiles de Smart Client) ... 490
Pestaña Reproducción (perfiles de Smart Client) ... 491
Pestaña Configuración (perfiles de Smart Client) ... 491
Pestaña Exportaciones (perfiles de Smart Client) ... 491
Pestaña Línea de timepo (perfiles de Smart Client) ... 492
Pestaña Control de acceso (perfiles de Smart Client) ... 492
Pestaña Gestor de alarmas (perfiles de Smart Client) ... 492
Pestaña Plano inteligente (perfiles de Smart Client) ... 493
Management Client Perfiles (nodo Cliente) ... 494
Pestaña Información (Management Client Perfiles) ... 494
Pestaña Perfil (Perfiles de Management Client) ... 495
Navegación ... 495
Detalles ... 496
Menú de herramientas ... 497
Sitios federados ... 498
Nodo Reglas y eventos ... 498
Reglas (nodo Reglas y Eventos) ... 498
Recrear reglas predeterminadas ... 500
Perfiles de notificación (nodo Reglas y Eventos) ... 501
Descripción general de eventos ... 504
Hardware: ... 504
Hardware - Eventos configurables: ... 504
Hardware - Eventos predefinidos: ... 504
Dispositivos - Eventos configurables: ... 504
Dispositivos - Eventos predefinidos: ... 505
Eventos externos - Eventos predefinidos: ... 508

Eventos externos - Eventos genéricos: 509
Eventos externos - Eventos definidos por el usuario: 509
Servidores de grabación: 509
Eventos del monitor del sistema 511
Monitor del sistema - Servidor: 512
Monitor del sistema - Cámara: 513
Monitor del sistema - Disco: 514
Monitor del sistema - Almacenamiento: 515
Otro: 515
Eventos de productos e integraciones adicionales: 516
Acciones y acciones de parada 516
Asistente de gestión de reglas 516
Probar evento de análisis (propiedades) 530
Eventos genéricos y fuentes de datos (propiedades) 532
Evento genérico (propiedades) 532
Fuente de datos de eventos genéricos (propiedades) 534
Webhooks (nodo Reglas y Eventos) 536
Nodo Seguridad 537
Roles (nodo Seguridad) 537
Pestaña Información (roles) 537
Pestaña Usuario y Grupos (roles) 539
IDP externo (cometidos) 539
Pestaña Seguridad global (roles) 540
Pestaña Dispositivo (roles) 573
Permisos relacionados con la cámara 573
Permisos relacionados con el micrófono 576
Permisos relacionados con los altavoces 579
Permisos relacionados con los metadatos 582
Permisos relacionados con la entrada 585
Permisos relacionados con la salida 585
Pestaña PTZ (roles) 586
Pestaña Habla (roles) 587

Pestaña Grabaciones remotas (roles) 588
Smart Wall pestaña (funciones) 588
Pestaña Evento externo (roles) 588
Pestaña Grupo de vistas (roles) 589
Pestaña Servidores (roles) 589
Matrix pestaña (funciones) 590
Pestaña Alarmas (roles) 590
Pestaña Control de acceso (roles) 591
Pestaña LPR (roles) 591
Pestaña Inicdentes (roles) 592
MIP pestaña (funciones) 592
Usuario básico (nodo Seguridad) 593
Nodo Panel del sistema 593
Nodo Panel del sistema 593
Tareas actuales (nodo Panel de control del sistema) 594
Monitor del sistema (nodo Panel del sistema) 594
Ventana del panel del monitor del sistema 594
Mosaicos 594
Lista de hardware con parámetros de monitorización 595
Personalizar ventana del panel de control 595
Ventana Detalles 595
Umbrales del monitor del sistema (nodo Panel del sistema) 597
Bloqueo de evidencias (nodo Panel de control del sistema) 600
Informes de configuración (nodo Panel de control del sistema) 600
Nodo Registros del servidor 601
Nodo Registros del servidor 601
Registros del sistema (pestaña) 601
Registros de auditoría (pestaña) 602
Registros desencadenados por reglas (pestaña) 603
Nodo de uso de metadatos 603
Metadatos y búsqueda de metadatos 603
¿Qué son metadatos? 603

Búsqueda de metadatos ... 604
Requisitos de la búsqueda de metadatos ... 604
Nodo de control de acceso ... 604
Propiedades de control de acceso ... 604
Pestaña configuración general (control de acceso) ... 604
Pestaña de puertas y cámaras asociadas (control de acceso) ... 606
Pestaña de eventos de control de acceso (control de acceso) ... 607
Pestaña de notificación de solicitud de acceso (control de acceso) ... 608
Pestaña de poseedores de tarjetas (control de acceso) ... 609
Nodo de incidentes ... 610
Propiedades del incidente (nodo Incidentes) ... 610
Nodo de transacción ... 611
Fuentes de transacciones (nodo Transacción) ... 611
Fuentes de transacción (propiedades) ... 611
Definiciones de transacciones (nodo Transacción) ... 612
Definiciones de transacciones (propiedades) ... 613
Nodo de alarmas ... 616
Definiciones de alarmas (nodo Alarmas) ... 616
Ajustes de definición de alarmas: ... 616
Desencadenante de alarmas: ... 617
Acción del opreador requerida: ... 617
Planos: ... 617
Otro: ... 618
Ajustes de datos de alarmas (nodo Alarmas) ... 619
Pestaña Niveles de datos de alarmas ... 619
Estados ... 619
Pestaña Motivos para el cierre ... 620
Ajustes de sonido (nodo Alarmas) ... 620
Jerarquía de sitios federados ... 621
Propiedades de sitio federado ... 621
Pestaña general ... 621
Pestaña del sitio principal ... 622

Copyright, marcas comerciales y exención de responsabilidad

Marcas comerciales

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

Microsoft y Windows son marcas comerciales registradas de Microsoft Corporation. App Store es una marca de servicios de Apple Inc. Android es una marca registrada 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 de hacer modificaciones sin notificación previa.

Todos los nombres de personas y organizaciones utilizados en los ejemplos de este documento son ficticios. Todo parecido con cualquier persona física, en vida o fallecida, o jurídica real es pura coincidencia y carece de intencionalidad alguna.

Este producto podrá hacer uso de software de terceros, respecto del cual es posible que sean de aplicación condiciones propias. Si ese es el caso, encontrará más información en el archivo `3rd_party_software_terms_and_conditions.txt`, que se encuentra en la carpeta de instalación de su sistema Milestone.

Generalidades

Novedades

En Management Client 2023 R1

XProtect Incident Manager:

- Par cumplir con el RGPD u otras leyes aplicables relativas a los datos personales, ahora los administradores de XProtect Management Client pueden definir un periodo de retención para proyectos de incidentes.

En Management Client 2022 R3

XProtect Incident Manager:

- El complemento de XProtect Incident Manager ahora también es compatible con XProtect Expert, XProtect Professional+ y XProtect Express+, versión 2022 R3 o posteriores.
- XProtect Incident Manager ahora puede mostrar más de 10 000 proyectos de incidentes.

En Management Client 2022 R2

XProtect Incident Manager:

- La primera versión de este add-on
- El add-on de XProtect Incident Manager es compatible con la versión 2022 R2 y posteriores de XProtect Corporate, y con la versión 2022 R2 y posteriores de XProtect Smart Client.

XProtect LPR:

- Los estilos de matrícula que forman parte de módulos de país ahora se recogen en un lugar.
- Para hacer que los estilos de matrícula sean más fáciles de manejar, puede agruparlos en alias en función de sus necesidades de reconocimiento de matrículas.
- Las listas de coincidencia de matrículas ahora son compatibles con los alias.

En Management Client 2022 R1

Cifrado del servidor de eventos:

- Puede cifrar la conexión bidireccional entre el servidor de eventos y los componentes que se comunican con el servidor de eventos, incluyendo el LPR Server.

  Si desea más información, consulte Habilitar el cifrado del servidor de eventos en la página 313.

Acceso a través de un IDP externo:

- Ahora puede iniciar sesión en el Milestone XProtect VMS utilizando un IDP externo. El inicio de sesión a través de un IDP externo es una alternativa al inicio de sesión como usuario de Active Directory o como usuario básico. Con el método de inicio de sesión del IDP externo puede eludir los requisitos de configuración de un usuario básico y seguir teniendo autorización para acceder a los componentes y dispositivos en XProtect.

  Para obtener más información, consulte el PDI externo (explicación).

Actualizar datos de hardware

- Ahora puede ver la versión actual del firmware para el dispositivo de hardware que detecta el sistema en el Management Client.

  Si desea más información, consulte Actualizar los datos de su hardware en la página 359.

XProtect Management Server Failover

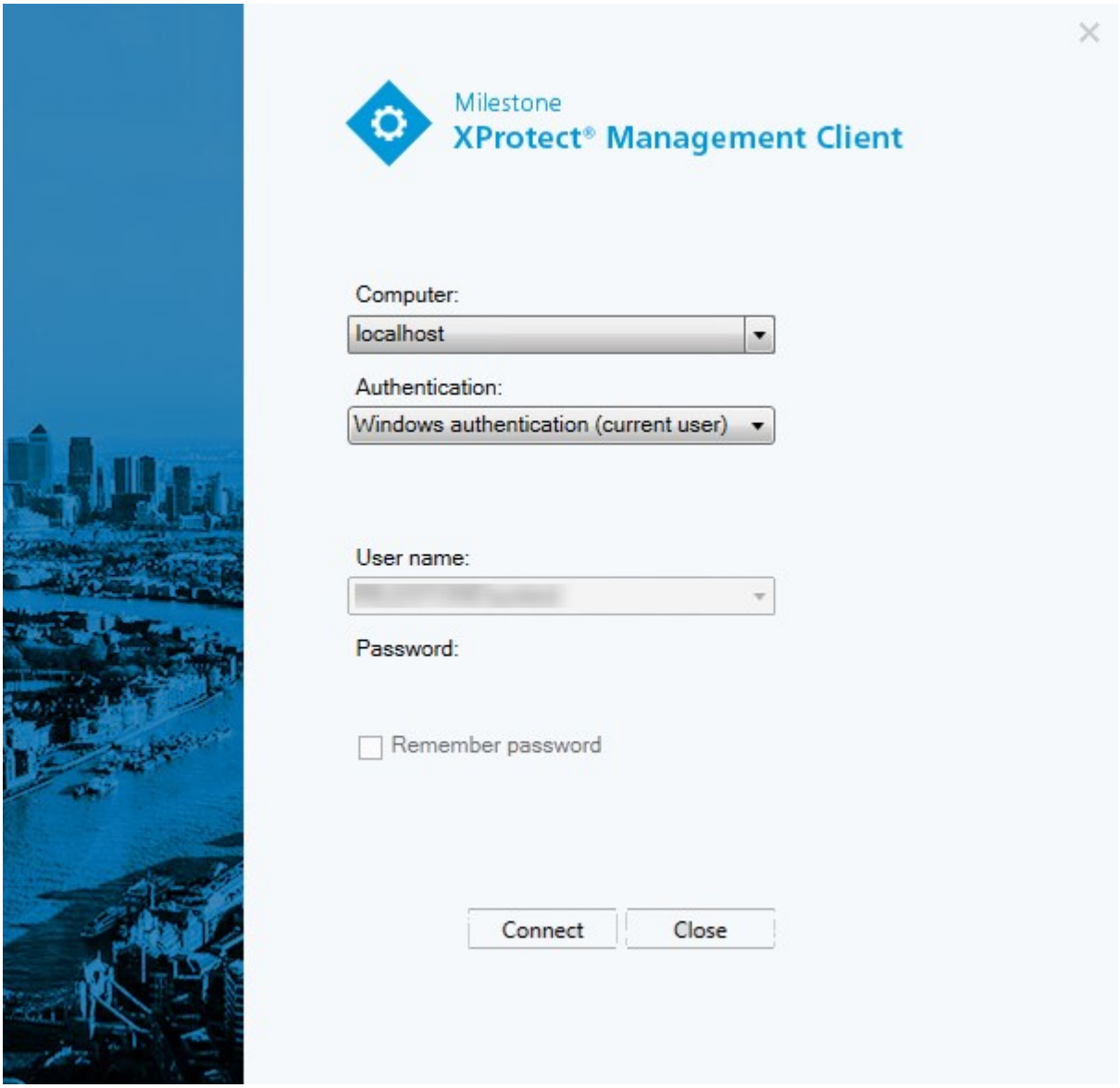
- Ahora puede conseguir una alta disponibilidad de su sistema configurando un servidor de gestión de failover entre dos ordenadores redundantes. Si el ordenador que ejecuta el servidor de gestión falla, el segundo lo sustituye. La replicación de datos en tiempo real garantiza que las bases de datos del servidor de gestión, del servidor de registro y del servidor de eventos sean idénticas en ambos ordenadores.

  Si desea más información, consulte XProtect Management Server Failover en la página 36.

Iniciando sesión (explicación)

Cuando inicie Management Client, primero debe introducir su información de inicio de sesión para conectarse a un sistema.

Con XProtect Corporate 2016 , XProtect Expert 2016 o una versión más reciente instalada, puede iniciar sesión en sistemas que ejecuten versiones antiguas del producto después de instalar un parche. Las versiones permitidas son XProtect Corporate 2013 y XProtect Expert 2013 o más reciente.



Autorización adicional (explicación)

El sistema permite a los administradores configurar a los usuarios para que solo puedan iniciar sesión en un sistema si un segundo usuario con permisos suficientes autoriza su acceso. En este caso, XProtect Smart Client o el Management Client piden la segunda autorización durante el inicio de sesión.

Un usuario asociado al rol de **Administradores** integrados siempre tiene permisos para autorizar y no se le pide un segundo inicio de sesión, a menos que el usuario esté asociado a otro rol que requiera un segundo inicio de sesión.

Los usuarios que inicien sesión a través de un IDP externo no pueden configurarse con el requisito de ser autorizados por un segundo usuario.

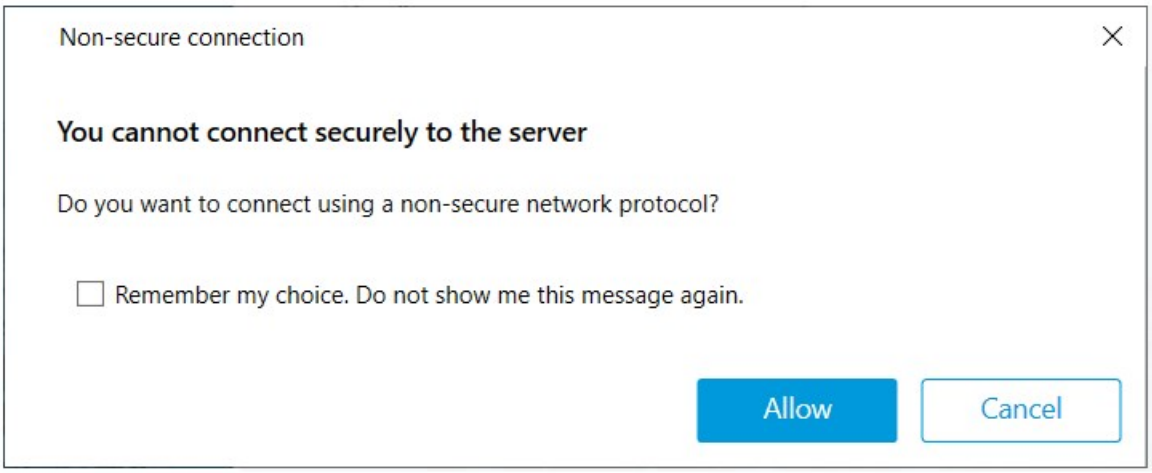
Para asociar la autorización de inicio de sesión a un rol:

- Establezca **Autorización de inicio de sesión requerido** para el rol seleccionado en la pestaña **Información** (consulte Ajustes de roles) en **Roles** para que se pida al usuario una autorización adicional durante el inicio de sesión
- Establezca **Autorizar usuarios** para el rol seleccionado en la pestaña **Seguridad general** (consulte Ajustes de roles) en **Roles**, para que el usuario pueda autorizar los inicios de sesión de otros usuarios

Puede elegir ambas opciones para el mismo usuario. Esto quiere decir que se pide al usuario autorización adicional durante el inicio de sesión, pero también puede autorizar inicios de usuario de otros usuarios, excepto el suyo propio.

Iniciar sesión utilizando una conexión no segura

Cuando inicia sesión en Management Client, es posible que se pregunte si quiere iniciar sesión utilizando un protocolo de red no seguro.



- Haga clic en **Permitir** para iniciar sesión sin tener en cuenta la notificación. Para evitar recibir esta notificación en el futuro, seleccione **Recordar mi elección. No volver a mostrarme este mensaje** o haga clic en **Herramientas** > **Opciones** y, a continuación, seleccione **Permitir conexión no segura al servidor (requiere reiniciar Management Client)**.

Para obtener información sobre comunicación segura, consulte Comunicación segura (explicación) en la página 150.

Cambiar su contraseña de usuario básico

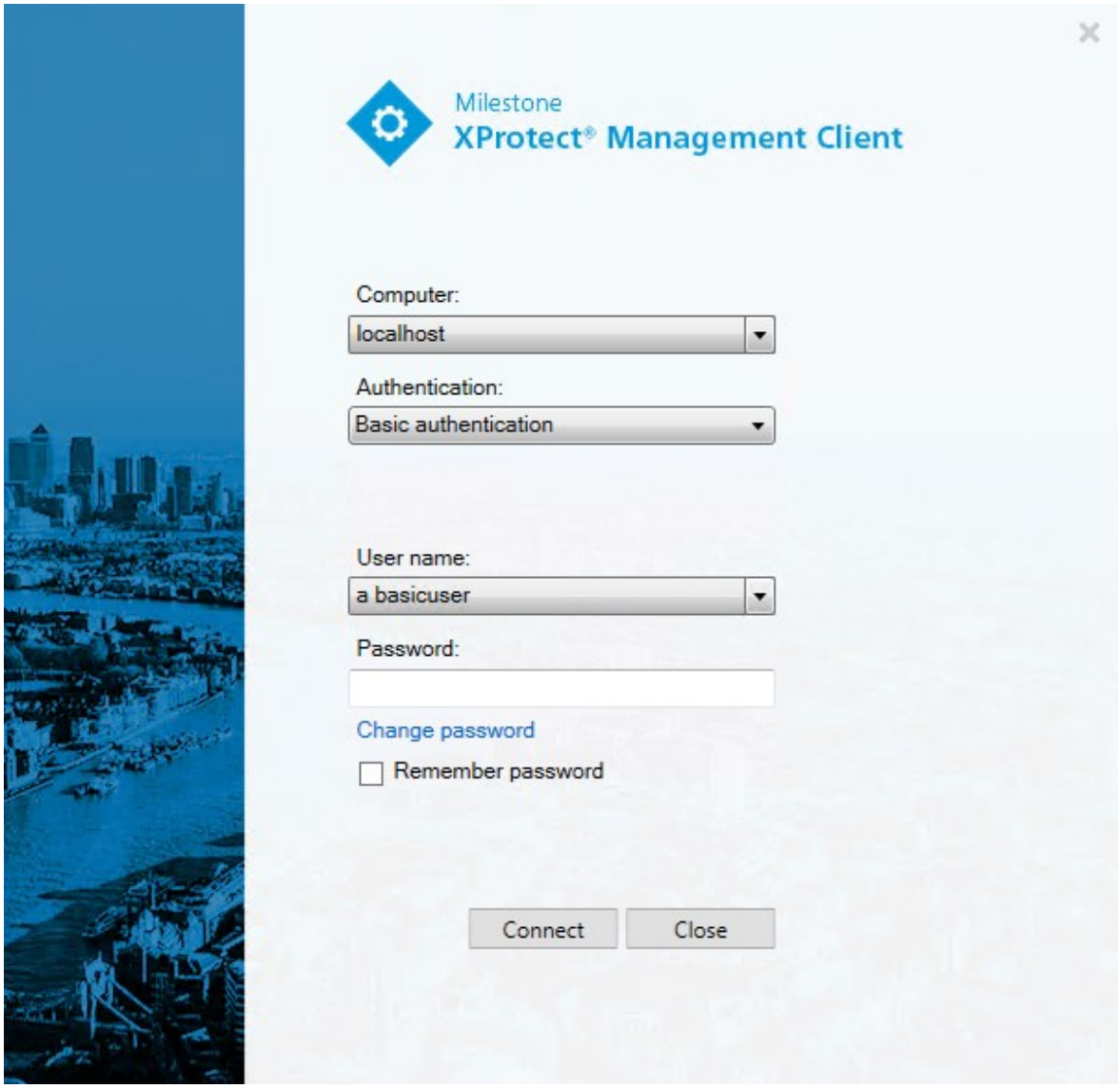
Si inicia sesión como un **Usuario básico**, puede cambiar su contraseña. Si elige un método de autenticación diferente, sólo el administrador del sistema puede cambiar su contraseña. Cambiar la contraseña con frecuencia aumenta la seguridad de su sistema VMS XProtect.

Requisitos

La versión de su sistema VMS de XProtect debe ser 2021 R1 o posterior.

Pasos:

1. Inicio Management Client. La ventana de inicio de sesión se abre.
2. Especifique su información de acceso. En la lista de **Autenticación**, seleccione **Autenticación básica**. Aparece un enlace con el texto **Cambiar contraseña**.



3. Haga clic en el enlace. Se abre una ventana del navegador.
4. Siga las instrucciones y guarde los cambios.
5. Ahora puede iniciar sesión en Management Client utilizando su contraseña nueva.

Descripción general del producto

Los productos de XProtect VMS son programas de software de gestión de vídeo diseñados para instalaciones de todas las formas y tamaños. Si quiere proteger su almacenamiento frente actos de vandalismo o quiere manejar una instalación de alta seguridad en varios sitios, XProtect hace que sea posible. Las soluciones

ofrecen gestión centralizada de todos los dispositivos, servidores y usuarios, y proporcionan un sistema de reglas extremadamente flexible impulsado por calendarios y eventos.

El sistema consta de los siguientes componentes principales:

- El **servidor de gestión**, el centro de su instalación, consta de múltiples servidores
- Uno o más **servidores de grabación**
- Una o más instalaciones de **XProtect Management Client**
- **XProtect Download Manager**
- Una o más instalaciones de **XProtect® Smart Client**
- Uno o más usos de **XProtect Web Client** y/o instalaciones del cliente de **XProtect Mobile** en caso necesario

El sistema también incluye funcionalidad totalmente integrada de Matrix para la visualización distribuida de vídeo desde cualquier cámara en su sistema de vigilancia en cualquier ordenador que tenga XProtect Smart Client instalado.

Puede instalar su sistema en servidores virtualizados o en varios servidores físicos en una configuración distribuida. Consulte también Una configuración de sistema distribuida en la página 91.

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

Con la mayoría de productos ricos en características instalados (consulte Comparación de productos en la página 116), su sistema puede manejar un número ilimitado de cámaras, servidores y usuarios en múltiples sitios en caso necesario. El sistema puede manejar IPv4 así como IPv6.

Componentes del sistema

Servidor de gestión (explicación)

El servidor de gestión es el componente central del sistema VMS. Almacena la configuración del sistema de vigilancia en una base de datos SQL, ya sea en un SQL Server en el propio ordenador del servidor de gestión o en un SQL Server separado en la red. También se encarga de la autentificación de los usuarios, los permisos de los usuarios, el sistema de reglas y mucho más. Para mejorar el rendimiento del sistema, puede ejecutar varios servidores de gestión como un Milestone Federated Architecture™. El servidor de gestión se ejecuta en como un servicio y normalmente se instala en un servidor dedicado.

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

Instalaciones SQL Server y bases de datos (explicación)

El servidor de gestión, el servidor de eventos y el servidor de registros almacenan, por ejemplo, la configuración del sistema, alarmas, eventos y mensajes de registro en bases de datos SQL en una o más instalaciones de SQL Server. El servidor de gestión y el de eventos comparten la misma base de datos SQL, mientras que el servidor de registro , XProtect Incident Manager, y el Identity Provider tienen cada uno su propia base de datos SQL. Para obtener más información sobre el Identity Provider, consulte Identity Provider (explicación) en la página 65. Para obtener más información sobre la base de datos XProtect Incident Manager SQL y el acceso, consulte el manual independiente de administrador para XProtect Incident Manager

El instalador del sistema incluye Microsoft SQL Server Express que es una edición gratuita de SQL Server.

Para sistemas muy grandes o con muchas transacciones hacia y desde las bases de datos SQL, Milestone recomienda utilizar una edición del Microsoft® SQL Server® Standard o Microsoft® SQL Server® Enterprise de SQL Server en un ordenador dedicado en la red y en un disco duro dedicado que no se utilice para otros fines. La instalación del SQL Server en su propia unidad mejora el rendimiento de todo el sistema.

Servidor de grabación (explicación)

El servidor de grabaciones es responsable de comunicarse con las cámaras y los codificadores de vídeo de la red, grabar el vído y el audio recuperados, así como de proporcionar acceso al cliente tanto para audio y vídeo en directo como grabado. El servidor de grabaciones también es responsable de comunicarse con otros productos de Milestone conectados mediante la tecnología Milestone Interconnect.

Controladores de dispositivos

- Las cámaras de red y los codificadores de vídeo se comunican a través de un controlador de dispositivos desarrollado específicamente para dispositivos individuales o una serie de dispositivos similares del mismo fabricante
- Desde la versión 2018 R1, los controladores de dispositivos se dividen en dos paquetes de dispositivos: el paquete de dispositivos normal con controladores más recientes y un paquete de dispositivo existente con controladores antiguos
- El paquete de dispositivos normal se instala automáticamente al instalar el servidor de grabación. Más adelante, puede actualizar los controladores descargando e instalando una versión más reciente del paquete del dispositivo
- El paquete de dispositivos heredados solo puede instalarse si el sistema tiene instalado un paquete de dispositivos normal. Los drivers del paquete de dispositivos heredados se instalan automáticamente si ya hay una versión anterior instalada en su sistema. Está disponible para su descarga e instalación manuales en la página de descargas de software (https://www.milestonesys.com/downloads/)

Base de datos de medios

- El servidor de grabaciones almacena los datos de audio y vídeo recuperados en la base de datos de medios de alto rendimiento y personalizada, optimizada para grabar datos de audio y vídeo
- La base de datos de medios admite varias características únicas como archivado en múltiples etapas, arreglos de vídeo, encriptación y adición de firma digital a las grabaciones

El sistema utiliza servidores de grabación para grabar los flujos de vídeo y para comunicarse con las cámaras y otros dispositivos. Un sistema de vigilancia suele estar formado por varios servidores de grabación.

Los servidores de grabación son ordenadores en los que se ha instalado el software Recording Server y se ha configurado para que se comunique con el servidor de gestión. Podrá ver sus servidores de grabación en el panel de **Generalidades** cuando expanda la carpeta **Servidores** y luego seleccione **Servidores de grabación**.

La compatibilidad con versiones del servidor de grabación anteriores a esta versión del servidor de gestión es limitada. Puede seguir accediendo a las grabaciones de los servidores de grabación con versiones anteriores, pero si quiere cambiar su configuración, asegúrese de que coinciden con esta versión del servidor de gestión. Milestone recomienda que actualice todos los servidores de grabación de su sistema a la misma versión que el servidor de gestión.

El servidor de grabación admite el cifrado de los flujos de datos hacia los clientes y los servicios:

- Habilitar encriptación en clientes y servidores en la página 315
- Ver el estado del cifrado a los clientes en la página 299

El servidor de grabación también admite el cifrado de la conexión con el servidor de gestión:

- Habilitar encriptación en y desde el servidor de gestión en la página 309

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

- Añadir hardware en la página 217
- Mover el hardware en la página 352
- Eliminar todo el hardware de un servidor de grabación en la página 373
- Eliminar un servidor de grabación en la página 372

> ⚠ Cuando el servicio de Recording Server se está ejecutando, es muy importante que el explorador de Windows u otros programas no accedan a archivos o carpetas de bases de datos de medios asociados a la configuración de su sistema. Si lo hacen, es probable que el servidor de grabación no pueda cambiar el nombre o mover archivos de medios relevantes. Esto podría provocar la para del servidor de grabaciones. Para reiniciar un servidor de grabación detenido, detenga el servicio Recording Server, cierre el programa accediendo a los archivos o carpetas de medios relevantes y reinicie el servicio Recording Server.

Servidor móvil (explicación)

El servidor móvil es responsable de dar al cliente de XProtect Mobile y a los usuarios de XProtect Web Client acceso al sistema.

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

Si está realizando una instalación **Distribuida** o **Personalizada**, Milestone recomienda que el servidor móvil se instale en un servidor dedicado.

Servidor de eventos (explicación)

El servidor de eventos maneja varias tareas relacionados con eventos, alarmas y planos y quizás también integraciones de terceros por medio de MIP SDK.

Eventos

- Todos los eventos del sistema están consolidados en el servidor de eventos, de modo que hay un lugar y una interfaz para realizar integraciones que utilizan eventos del sistema
- Además, el servidor de eventos ofrece acceso a terceros para enviar eventos al sistema mediante la interfaz de Eventos genéricos o Eventos de análisis

Alarmas

- El servidor de eventos alberga la característica de la alarma, la lógica de la alarma, el estado de la alarma, además de manejar la base de datos de alarmas. La base de datos de alarmas se almacena en la misma base de datos de SQL que utiliza el servidor de gestión

Planos

- El servidor de eventos también alberga los planos en los que están configurados y se usan en XProtect Smart Client

MIP SDK

- Finalmente, los plug-ins desarrollados por terceros se pueden instalar en el servidor de eventos y utilizan el acceso a los eventos del sistema

Servidor de registros (explicación)

El servidor de registro almacena todos los mensajes de registro para todo el sistema en una base de datos SQL. Esta base de datos SQL de mensajes de registro puede existir en el mismo SQL Server que la base de datos SQL de configuración del sistema del servidor de gestión o en un SQL Server separado. El servidor de registros normalmente se instala en el mismo servidor que el servidor de gestión, pero se puede instalar en un servidor independiente para un mayor rendimiento de los servidores de gestión y registro.

API Gateway (explicación)

El MIP VMS API proporciona una API de RESTful unificada, basada en protocolos estándar de la industria, como OpenAPI, para acceder a la funcionalidad de XProtect VMS, lo que simplifica los proyectos de integración y sirve como base para la comunicación conectada a la nube.

El XProtect VMS API Gateway es compatible con estas opciones de integración por medio del Milestone Integration Platform VMS API (MIP VMS API).

El API Gateway está instalado localmente y tiene como finalidad servidor como front-end y punto de entrada común para servicios de API de RESTful en todos los componentes del servidor VMS actual (servidor de gestión, servidor de eventos, servidores de grabaciones, servidor de registros, etc.). Puede haber un servicio de API Gateway instalado en el mismo host que el servidor de gestión o de forma individual, y se puede instalar más de uno (cada uno en su propio host).

La implementación de la API de RESTful se realiza en parte por cada componente del servidor VMS específico, y el API Gateway simplemente puede canalizar estas solicitudes y respuestas, mientras que, para otras solicitudes, el API Gateway convertirá solicitudes y respuestas según sea necesario.

Actualmente, la API de configuración, alojada por el servidor de gestión, está disponible como una API de RESTful.

Para obtener más información, consulte el manual de usuario de API Gateway y la documentación de referencia de Milestone Integration Platform VMS API.

Failover

XProtect Management Server Failover

Si un ordenador independiente que esté ejecutando el servicio Management Server o el SQL Server tiene un fallo de hardware, esto no afecta a las grabaciones ni al servidor de grabación. Sin embargo, estos fallos de hardware pueden provocar un tiempo de inactividad para operadores y administradores que no hayan iniciado sesión en los clientes.

XProtect Management Server Failover proporciona una gran visibilidad y recuperación de desastres para el servidor de gestión. Si el servidor de gestión deja de estar disponible en un ordenador, el otro se encarga de ejecutar los componentes del sistema.

Opcionalmente, puede utilizar la replicación segura en tiempo real de las bases de datos de SQL Server. De esta forma, se asegurará de que no haya pérdida de datos en caso de fallos de hardware.

XProtect Management Server Failover puede ayudarle a mitigar el tiempo de inactividad del sistema. Puede beneficiarse de un clúster de conmutación por error cuando:

- Un servidor falla: puede ejecutar el servicio Management Server y SQL Server desde otro ordenador mientras resuelve los problemas.
- Necesita aplicar actualizaciones del sistema y parches de seguridad: aplicar parches de seguridad en un servidor de gestión independiente puede requerir mucho tiempo, lo que provoca periodos de inactividad prolongados. Cuando tiene un clúster de conmutación por error, puede aplicar actualizaciones del sistema y parches de seguridad con un tiempo de inactividad mínimo.
- Necesita una conexión perfecta: los usuarios obtienen acceso continuo a vídeo en directo y reproducción, y a la configuración del sistema en todo momento.

Puede configurar XProtect Management Server Failover entre dos ordenadores. Para que la conmutación por error funcione, se instalará en cada ordenador:

- XProtect Management Server
- Servicio XProtect Event Server
- Servicio XProtect Log Server
- Microsoft SQL Server (opcional)

Servidor de gestión de failover (explicación)

El soporte de failover en el servidor de gestión se logra instalando el servidor de gestión en un clúster de Microsoft Windows. El clúster garantizará entonces que otro servidor asuma la función del servidor de gestión en caso de que el primer servidor falle.

Servidor de grabación de failover (explicación)

> La funcionalidad disponible depende del sistema que esté utilizando. Vea la lista completa de características, que está disponible en la página de descripción del producto en el sitio web Milestone (https://www.milestonesys.com/solutions/platform/product-index/).

Un servidor de grabación de failover es un servidor de grabación adicional que sustituye al servidor de grabación estándar si éste no está disponible. Puede configurar un servidor de grabación de failover en dos modos, como **servidor de espera en frío** o como **servidor de espera en caliente**.

Los servidores de grabación failover se instalan como los servidores de grabación estándar (consulte Instalar un servidor de grabación de failover a través de Download Manager en la página 175). Una vez que haya instalado los servidores de grabación de failover, serán visibles en el Management Client. Milestone recomienda que instale todos los servidores de grabación de failover en ordenadores separados. Asegúrese de configurar los servidores de grabación de failover con la dirección IP/nombre de host correctos del servidor de gestión. Los permisos de usuario para la cuenta de usuario bajo la que se ejecuta el servicio del servidor de failover se proporcionan durante el proceso de instalación. Estos son:

- Permisos de inicio/detención para iniciar o detener el servidor de grabación de failover
- Permisos de acceso de lectura y escritura para leer o escribir el archivo RecorderConfig.xml

Si se selecciona un certificado para el cifrado, el administrador debe conceder permiso de acceso de lectura al usuario de failover sobre la clave privada del certificado seleccionado.

Si el servidor de grabación de failover se hace cargo de un servidor de grabación que utiliza cifrado, Milestone recomienda preparar también el servidor de grabación de failover para que utilice el cifrado. Si desea más información, consulte Comunicación segura (explicación) en la página 150 y Instalar un servidor de grabación de failover a través de Download Manager en la página 175.

Puede especificar qué tipo de soporte de failover desea a nivel de dispositivo. Para cada dispositivo de un servidor de grabación, seleccione soporte completo, solo en directo o sin failover. Esto le ayuda a priorizar sus recursos de failover y, por ejemplo, a configurar solo el failover para el vídeo y no para el audio, o solo tener failover en las cámaras esenciales y no en las menos importantes.

Mientras el sistema está en modo de failover, no se puede reemplazar o mover el hardware, actualizar el servidor de grabación o cambiar las configuraciones de los dispositivos, como los ajustes de almacenamiento o de flujo de vídeo.

Servidores de grabación de failover en frío

En una configuración de servidor de grabación de failover en frío, se agrupan varios servidores de grabación de failover en un grupo de failover. Todo el grupo de failover está dedicado a hacerse cargo de cualquiera de los varios servidores de grabación preseleccionados, si uno de ellos deja de estar disponible. Puede crear tantos grupos como desee (consulte Servidores de grabación de failover en grupo para la espera en frío en la página 215).

La agrupación tiene una clara ventaja: cuando se especifica posteriormente qué servidores de grabación de failover deben tomar el relevo de un servidor de grabación, se selecciona un grupo de servidores de grabación de failover. Si el grupo seleccionado contiene más de un servidor de grabación de failover, este le ofrece la seguridad de tener más de un servidor de grabación de failover listo para tomar el relevo si un servidor de grabación no está disponible. Puede especificar un grupo de servidores de failover secundario que tome el relevo del grupo primario si todos los servidores de grabación del grupo primario están ocupados. Un servidor de grabación de failover solo puede ser miembro de un grupo a la vez.

Los servidores de grabación de failover en un grupo de failover se ordenan en una secuencia. La secuencia determina el orden en el que los servidores de grabación de failover se harán cargo de un servidor de grabación. Por defecto, la secuencia refleja el orden en el que ha incorporado los servidores de registro de failover en el grupo de failover: el primero en es el primero en la secuencia. Puede cambiarlo si lo necesita.

Servidores de grabación por failover en caliente

En una configuración de servidor de grabación de failover en caliente, se dedica un servidor de grabación de failover para encargarse solo de **un** servidor de grabación. Debido a esto, el sistema puede mantener este servidor de grabación de failover en 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 el relevo mucho más rápido que un servidor de grabación de failover en espera fría. Como se ha mencionado, asigna servidores de espera en caliente a un solo servidor de grabación y no se pueden agrupar. No puede asignar servidores de failover que ya formen parte de un grupo de failover como servidores de grabación de espera en caliente.

Validación del servidor de grabación de failover

Para validar una fusión de datos de vídeo desde el servidor de failover al servidor de grabación, debe hacer que el servidor de grabación no esté disponible deteniendo el servicio del servidor de grabación o apagando el ordenador del servidor de grabación.

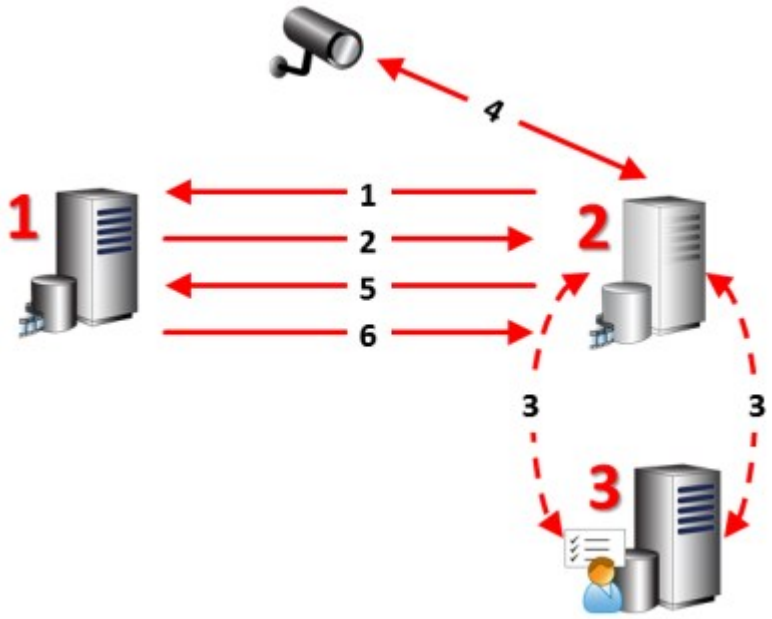
Cualquier interrupción manual de la red que pueda provocar tirando del cable de red o bloqueando la red con una herramienta de prueba no es un método válido.

Funcionalidad del servidor de grabación de failover (explicación)

- Un servidor de grabación de failover comprueba el estado de los servidores de grabación relevantes cada 0,5 segundos. Si un servidor de grabación no responde en 2 segundos, el servidor de grabación se considera no disponible y el servidor de grabación de failover se encarga de ello
- Un servidor de grabación de reserva fría sustituye al servidor de grabación que no está disponible después de cinco segundos más el tiempo que tarda en iniciarse el servicio del servidor de grabación de reserva de Recording Server y el tiempo que tarda en conectarse a las cámaras. Por el contrario, un servidor de grabación de failover en caliente se hace cargo más rápidamente porque el servicio Recording Server ya está en marcha con la configuración correcta y solo tiene que poner en marcha sus cámaras para entregar los contenidos. Durante el periodo de puesta en marcha, no se pueden almacenar grabaciones ni ver vídeo en directo de las cámaras afectadas
- Cuando un servidor de grabación vuelve a estar disponible, toma automáticamente el relevo desde el servidor de grabación failover. Las grabaciones almacenadas por el servidor de grabación de failover se fusionan automáticamente en las bases de datos del servidor de grabación estándar. El tiempo que se tarda en fusionar depende de la cantidad de grabaciones, la capacidad de la red y otros factores. Durante el proceso de fusión, no se pueden examinar las grabaciones del período durante el cual el servidor de grabación de failover se hizo cargo

- Si un servidor de grabación de failover debe sustituir a otro servidor de grabación durante el proceso de fusión en una configuración de servidor de grabación de failover en espera fría, pospone el proceso de fusión con el servidor de grabación A y sustituye al servidor de grabación B. Cuando el servidor de grabación B vuelve a estar disponible, el servidor de grabación de failover retoma el proceso de fusión y permite que tanto el servidor de grabación A como el servidor de grabación B fusionen las grabaciones simultáneamente.
- En una configuración de espera en caliente, un servidor de espera en caliente no puede encargarse de un servidor de grabación adicional porque solo puede estar en espera en caliente para un único servidor de grabación. Pero si ese servidor de grabación vuelve a fallar, la espera en caliente vuelve a tomar el relevo y mantiene las grabaciones del periodo anterior. El servidor de grabación mantiene las grabaciones hasta que se fusionan de nuevo con el grabador principal o hasta que el servidor de grabación de failover se queda sin espacio en disco
- Una solución de failover no proporciona una redundancia completa. Solo puede servir como una forma fiable de minimizar el tiempo de inactividad. Si un servidor de grabación vuelve a estar disponible, el servicio Failover Server se asegura de que el servidor de grabación esté preparado para volver a almacenar grabaciones. Solo entonces se devuelve la responsabilidad de almacenar las grabaciones al servidor de grabación estándar. Por tanto, una pérdida de grabaciones en esta fase del proceso es muy poco probable
- Los usuarios clientes apenas se dan cuenta de que un servidor de grabación de failover se hace cargo. Se produce una breve interrupción, normalmente de pocos segundos, en la que el servidor de grabación de failover se hace cargo. Durante esta interrupción, los usuarios no pueden acceder al vídeo del servidor de grabación afectado. Los usuarios de los clientes pueden reanudar la visualización de vídeo en directo tan pronto como el servidor de grabación de failover se haya hecho cargo. Como las grabaciones recientes se almacenan en el servidor de grabación de failover, pueden reproducirse grabaciones posteriores a la toma de posesión del servidor de grabación de failover. Los clientes no pueden reproducir grabaciones antiguas almacenadas solo en el servidor de grabación afectado hasta que ese servidor de grabación vuelva a funcionar y se haya hecho cargo del servidor de grabación de failover. No puede acceder a las grabaciones archivadas. Cuando el servidor de grabación vuelve a funcionar, se lleva a cabo un proceso de fusión durante el cual las grabaciones por error se vuelven a fusionar en la base de datos del servidor de grabación. Durante este proceso, no puede reproducir grabaciones del período durante el cual el servidor de grabación de failover se hizo cargo
- En una configuración de espera en frío, no es necesario configurar un servidor de grabación de failover como copia de seguridad de otro servidor de grabación de failover. Esto se debe a que se asignan grupos de failover y no se asignan servidores de grabación de failover particulares para tomar el relevo de servidores de grabación específicos. Un grupo de failover debe contener al menos un servidor de grabación de failover, pero se pueden añadir tantos servidores de grabación de failover como sea necesario. Si un grupo de failover contiene más de un servidor de grabación de failover, más de un servidor de grabación de failover puede tomar el control.
- En una configuración de espera en caliente, no puede configurar servidores de grabación de failover o servidores de espera en caliente como failover para un servidor de espera en caliente

Pasos de failover (explicación)



Descripción
Servidores implicados (números en rojo): 1. Recording Server 2. Failover Recording Server 3. Management Server
Pasos de failover para configuraciones de **Espera en frío**: 1. Para comprobar si se está ejecutando o no, un servidor de grabación de failover tiene una conexión TCP ininterrumpida con un servidor de grabación. 2. Esta conexión se interrumpe. 3. El servidor de grabación de failover solicita al servidor de gestión la configuración actual del servidor de grabación. El servidor de gestión envía la configuración solicitada, el servidor de grabación de failover recibe la configuración, inicia y comienza a grabar en nombre del servidor de grabación. 4. El servidor de grabación failover y la(s) cámara(s) correspondiente(s) intercambian datos de vídeo.

Descripción
5. El servidor de grabación de failover intenta continuamente restablecer la conexión con el servidor de grabación. 6. Cuando se restablece la conexión con el servidor de grabación, el servidor de grabación de failover se apaga y el servidor de grabación recupera los datos de vídeo (si los hay) grabados durante su tiempo de inactividad y los datos de vídeo se fusionan de nuevo en la base de datos del servidor de grabación.
Pasos de failover para configuraciones de **Espera en caliente**: 1. Para comprobar si se está ejecutando o no, un servidor de espera en caliente tiene una conexión TCP ininterrumpida con su servidor de grabación asignado. 2. Esta conexión se interrumpe. 3. Desde el servidor de gestión, el servidor de espera en caliente ya conoce la configuración actual de su servidor de grabación asignado y comienza a grabar en su nombre. 4. El servidor de espera en caliente y la(s) cámara(s) correspondiente(s) intercambian datos de vídeo. 5. El servidor de espera en caliente intenta continuamente restablecer la conexión con el servidor de grabación. 6. Cuando se restablece la conexión con el servidor de grabación y el servidor de espera en caliente vuelve al modo de espera en caliente, el servidor de grabación recupera los datos de vídeo (si los hay) grabados durante su tiempo de inactividad y los datos de vídeo se fusionan de nuevo en la base de datos del servidor de grabación.

Servicios de servidor de grabación de failover (explicación)

Un servidor de grabación de failover tiene dos servicios instalados:

- Un servicio Failover Server que maneja los procesos de toma de posesión del servidor de grabación. Este servicio está siempre en funcionamiento y comprueba constantemente el estado de los servidores de grabación correspondientes

- Un servicio Failover Recording Server que habilita al servidor de grabación de failover para que actúe como servidor de grabación.

  En una configuración de reserva fría, este servicio solo se inicia cuando es necesario, es decir, cuando el servidor de grabación de reserva fría de failover se hace cargo del servidor de grabación. El inicio de este servicio suele tardar un par de segundos, pero puede tardar más en función de la configuración de seguridad local y otros aspectos.
  En una configuración de espera en caliente, este servicio está siempre en funcionamiento, lo que permite que el servidor de espera en caliente tome el relevo más rápidamente que el servidor de grabación de failover en frío.

Clientes

Management Client (explicación)

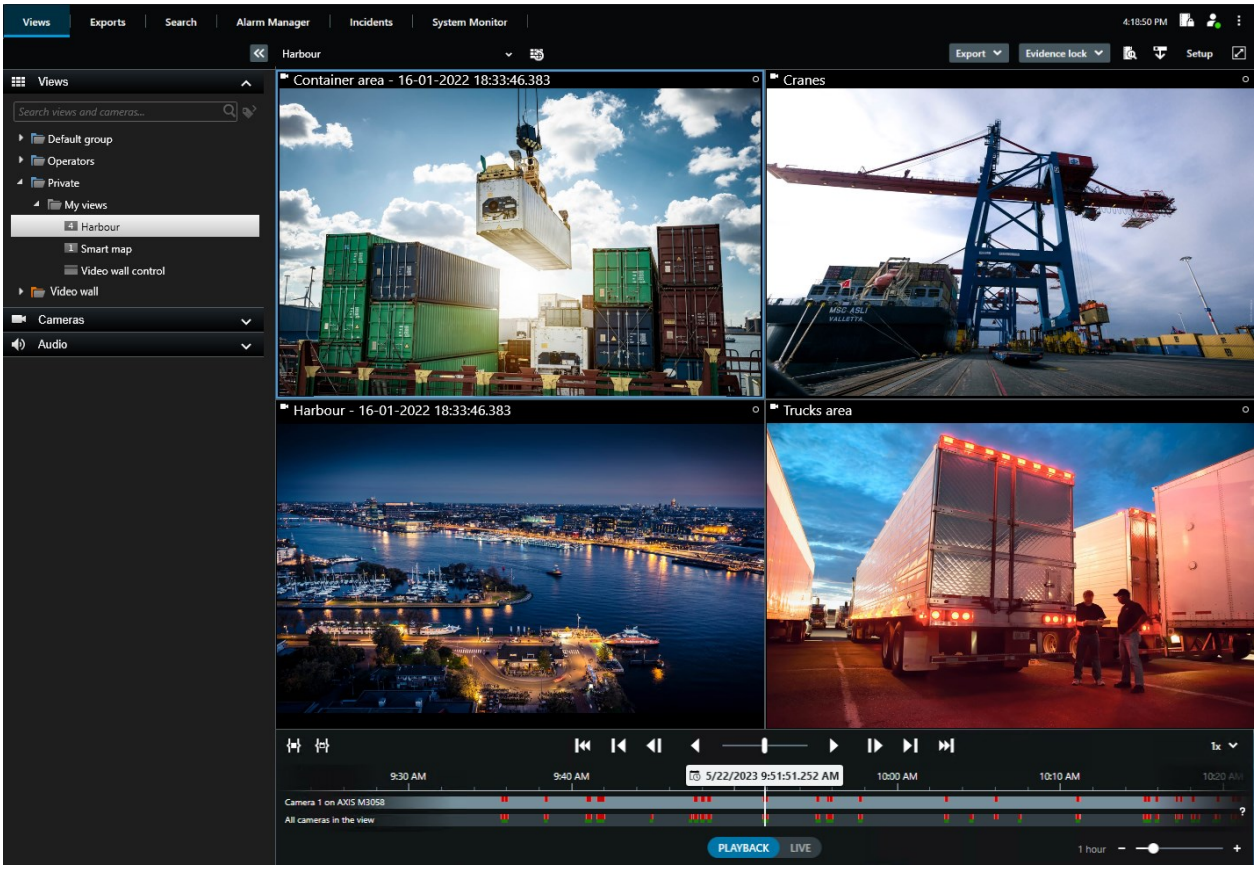
Management Client es un cliente de administración con muchas características para la configuración y la gestión diaria del sistema. Disponible en varios idiomas.

Normalmente instalado en la estación de trabajo del administrador del sistema de vigilancia o similar.

XProtect Smart Client (explicación)

XProtect Smart Client es una aplicación de escritorio diseñada para ayudarle a gestionar sus cámaras de vigilancia IP. Proporciona control intuitivo a través de instalaciones de seguridad brindando a los usuarios acceso a video en directo y grabado, control instantáneo de cámaras y dispositivos de seguridad conectados, y la capacidad de realizar búsquedas avanzadas para grabaciones y metadatos.

Disponible en varios idiomas locales, XProtect Smart Client tiene una interfaz de usuario adaptable que puede ser optimizada para las tareas de los operadores individuales y ser ajustada de acuerdo con habilidades específicas y niveles de autoridad.



La interfaz le permite personalizar su experiencia visual a entornos de trabajo específicos seleccionando un tema claro u oscuro. También dispone de pestañas optimizadas para trabajar y una línea temporal principal integrada para una fácil operación de vigilancia.

Utilizando la MIP SDK, los usuarios pueden integrar varios tipos de sistemas de seguridad y sistemas de negocios y aplicaciones de análisis de vídeo, que usted administra a través de XProtect Smart Client..

XProtect Smart Client debe ser instalada en los ordenadores de los operadores. Los administradores de sistemas de vigilancia administran el acceso al sistema de vigilancia a través de Management Client. Las grabaciones que ven los clientes son proporcionadas por el servicio XProtect de su sistema Image Server. El servicio se ejecuta en el fondo en el servidor del sistema de vigilancia. No se requiere hardware por separado.

XProtect Mobile cliente (explicación)

XProtect Mobile cliente es una solución de vigilancia móvil estrechamente integrada con el resto de su sistema XProtect. Se ejecuta en su tableta o teñlefono inteligente Android o en su tableta, teléfono inteligente o reproductor de música portátil de Apple® y le da acceso a cámaras, vistas y a la configuración de otras funcionalidades en los clientes de gestión.

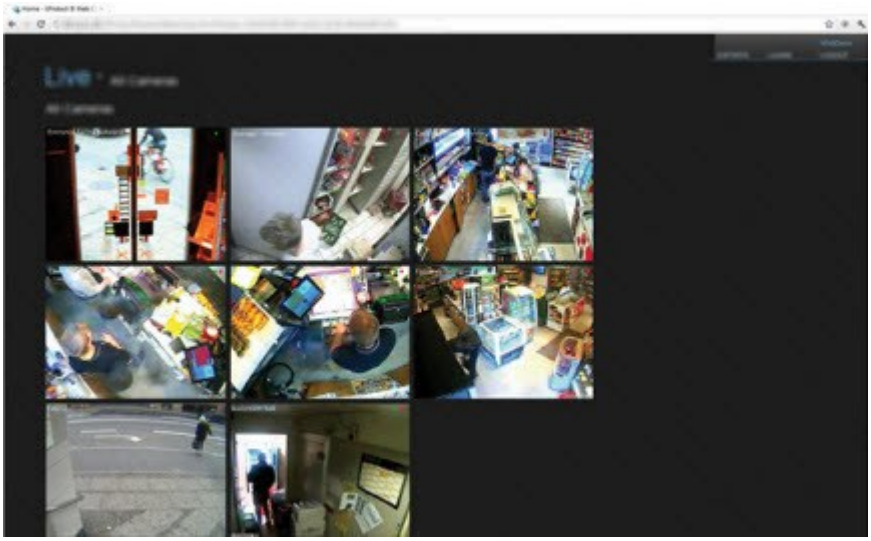
Utilice el cliente de XProtect Mobile para ver y reproducir un vídeo en directo y grabado desde una o varias cámaras, controlar cámaras de panorámica-inclinación-zoom (PTZ), desencadenar salidas y eventos, y utilizar la funcionalidad de envío automático de vídeo para enviar vídeo desde su dispositivo a su sistema XProtect.

Si quiere usar el cliente de XProtect Mobile con su sistema, debe tener un servidor de XProtect Mobile para establecer la conexión entre el cliente de XProtect Mobile y su sistema. Una vez configurado el servidor de XProtect Mobile, descargue el cliente de XProtect Mobile sin coste de Google Play o App Store para empezar a usar XProtect Mobile.

Necesita una licencia de dispositivo por dispositivo que debe ser capaz de enviar vídeo automáticamente a su sistema de XProtect.

XProtect Web Client (explicación)

XProtect Web Client es una aplicación cliente basada en la web para visualizar, reproducir y compartir vídeo. Proporciona acceso instantáneo a las funciones de vigilancia utilizadas con más frecuencia, como visualizar vídeo en directo, reproducir vídeo grabado, imprimir y exportar evidencia. El acceso a las funciones depende de los permisos individuales de los usuarios, que se configuran en Management Client.



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

Productos add-on

XProtect Access (explicación)

Milestone ha desarrollado productos add-on que se integran completamente XProtect para darle una funcionalidad extra. Su archivo de licencia de XProtect controla el acceso a productos add-on.

Para el uso de XProtect Access es necesario haber adquirido una licencia básica que le permita acceder a esta característica dentro del 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 proporcionados por proveedores en los casos en que ya exista un plug-in específico del proveedor para XProtect Access.

La función de integración del control de acceso introduce una nueva funcionalidad que facilita la integración de los sistemas de control de acceso de los clientes con XProtect. Obtiene:

- Una interfaz de usuario común para los sistemas de control de acceso múltiple en XProtect Smart Client
- Integración más rápida y potente de los sistemas de control de acceso
- Más funcionalidades para el operador (ver más abajo)

En XProtect Smart Client, el operador obtiene:

- Monitorización en directo de los eventos en los puntos de acceso
- Paso asistido por operador para las solicitudes de acceso
- Integración en plano
- Definiciones de alarmas para eventos de control de acceso
- Investigación de eventos en los puntos de acceso
- Visión general y control centralizados de los estados de las puertas
- Información y gestión de los poseedores de tarjetas

El **registro de auditoría** registra los comandos que cada usuario ejecuta en el sistema de control de acceso de XProtect Smart Client.

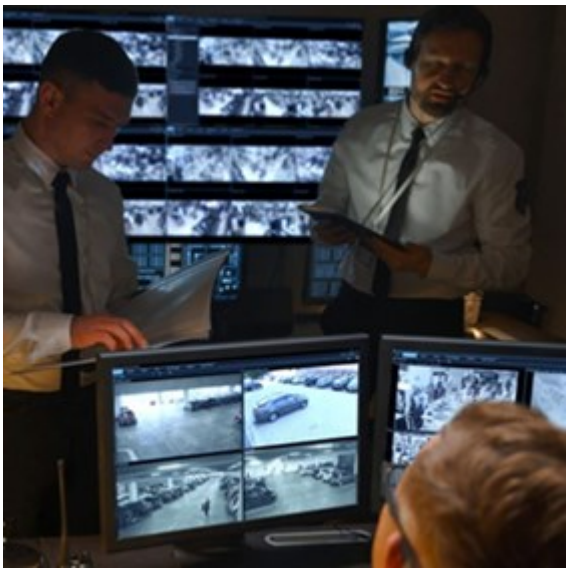
Aparte de una licencia básica XProtect Access, necesita un plug-in de integración específico del proveedor instalado en el servidor de eventos antes de poder iniciar una integración.

XProtect Incident Manager

Milestone ha desarrollado productos add-on que se integran completamente XProtect para darle una funcionalidad extra. Su archivo de licencia de XProtect controla el acceso a productos add-on.

> La funcionalidad disponible depende del sistema que esté utilizando. Vea la lista completa de características, que está disponible en la página de descripción del producto en el sitio web Milestone (https://www.milestonesys.com/solutions/platform/product-index/).

XProtect Incident Manager es un add-on de Milestone que habilita a las organizaciones para que documenten incidentes y los combinen con evidencias de secuencias (vídeo y posiblemente audio) desde su instalación VMS de XProtect.



Los usuarios de XProtect Incident Manager pueden guardar toda la información del incidente en proyectos de incidentes. Desde los proyectos de incidentes, pueden hacer un seguimiento del estado y de las actividades de cada incidente. De este modo, los usuarios pueden gestionar incidentes de manera efectiva y compartir fácilmente sólidas evidencias de incidentes, tanto internamente con colegas como externamente con autoridades.

XProtect Incident Manager ayuda a las organizaciones a tener una visión general y a comprender los incidentes que se producen en las áreas que vigilan. Este conocimiento habilita a las organizaciones para que implementen pasos orientados a minimizar la posibilidad de que en el futuro se produzcan incidentes similares.

En XProtect Management Client, los administradores del VMS de XProtect de una organización pueden definir las propiedades disponibles del incidente en XProtect Incident Manager según las necesidades de la organización. Los operadores de XProtect Smart Client inician, guardan y gestionan proyectos de incidentes, y añaden distinta información a los proyectos de incidentes. Esto incluye texto libre, propiedades del incidente que han definido los administradores y secuencias del VMS de XProtect. Para una trazabilidad completa, el VMS de XProtect registra cuándo los administradores definen y editan propiedades del incidente y cuándo los operadores crean y actualizan los proyectos de incidentes.

XProtect LPR (explicación)

Milestone ha desarrollado productos add-on que se integran completamente XProtect para darle una funcionalidad extra. Su archivo de licencia de XProtect controla el acceso a productos add-on.

La funcionalidad disponible depende del sistema que esté utilizando. Vea la lista completa de características, que está disponible en la página de descripción del producto en el sitio web Milestone (https://www.milestonesys.com/solutions/platform/product-index/).

XProtect LPR ofrece análisis de contenido basado en vídeo (VCA) y reconocimiento de matrículas de vehículos que interactúa con su sistema de vigilancia y su XProtect Smart Client.

Para leer los caracteres de una matrícula, XProtect LPR utiliza el reconocimiento óptico de caracteres en imágenes con la ayuda de ajustes especializados de la cámara.

Puede combinar el LPR (reconocimiento de matrículas) con otras funciones de vigilancia, como la grabación y la activación de salidas basada en eventos.

Ejemplos de eventos en XProtect LPR:

- Activar las grabaciones del sistema de vigilancia en una calidad determinada
- Activar alarmas
- Coincidencia con listas de coincidencia de matrículas positivas y negativas
- Abrir las puertas
- Encender las luces
- Transmisión de vídeos de incidentes a las pantallas de los ordenadores de determinados miembros del personal de seguridad
- Enviar mensajes de texto por teléfono móvil

Con un evento, se pueden activar alarmas en XProtect Smart Client.

XProtect Smart Wall (explicación)

Consulte también el manual de Smart Wall (https://doc.milestonesys.com/2023r2/es-ES/portal/htm/chapter-page-smart-wall.htm).

Milestone ha desarrollado productos add-on que se integran completamente XProtect para darle una funcionalidad extra. Su archivo de licencia de XProtect controla el acceso a productos add-on.

XProtect Smart Wall es una herramienta add-on avanzada que permite a las organizaciones crear paneles de vídeo que cumplan con sus demandas específicas de seguridad. XProtect Smart Wall proporciona una vista general de todos los datos de vídeo del sistema XProtect VMS[1] y admite cualquier cantidad o combinación de monitores

XProtect Smart Wall permite a los operadores ver paneles de vídeo estáticos definidos por el administrador del sistema con un conjunto fijo de cámaras y una distribución de monitores. Sin embargo, el panel de vídeo también está orientado al operador en el sentido de que éste puede controlar lo que se muestra. Esto incluye:

- Empujar cámaras y otros tipos de contenido al panel de vídeo, por ejemplo, imágenes, texto, alarmas y plano inteligente
- Envío de vistas completas a los monitores

[1]Abreviatura de "Video Management Software" (software de gestión de vídeo).

- En el transcurso de ciertos eventos, aplicar valores preestablecidos[1] alternativos

Por último, los cambios de visualización pueden ser controlados por reglas que cambian automáticamente los valores preestablecidos en función de eventos específicos o de horarios.

XProtect Transact (explicación)

Milestone ha desarrollado productos add-on que se integran completamente XProtect para darle una funcionalidad extra. Su archivo de licencia de XProtect controla el acceso a productos add-on.

> La funcionalidad disponible depende del sistema que esté utilizando. Vea la lista completa de características, que está disponible en la página de descripción del producto en el sitio web Milestone (https://www.milestonesys.com/solutions/platform/product-index/).

XProtect Transact es una adición a las soluciones de vigilancia de vídeo de IP de Milestone.

XProtect Transact es una herramienta para observar transacciones en curso y transacciones en investigación en el pasado. Las transacciones están enlazadas con el vídeo de vigilancia digital que monitoriza las transacciones, por ejemplo para ayudarle a demostrar fraudes o proporcionar evidencias ante una intrusión. Hay una relación de 1 a 1 entre las líneas de transacción e imágenes de vídeo.

Los datos de las transacciones pueden originarse en distintos tipos de fuentes de transacciones, normalmente sistemas de punto de venta (PoS) o cajeros automáticos (ATM).

Milestone Open Network Bridge (explicación)

Milestone ha desarrollado productos add-on que se integran completamente XProtect para darle una funcionalidad extra. Su archivo de licencia de XProtect controla el acceso a productos add-on.

Milestone Open Network Bridge es una interfaz abierta compatible con ONVIF para compartir vídeo estandarizado desde sistemas XProtect VMS con otros sistemas de seguridad basados en IP. Esto habilita a las fuerzas del orden, los centros de vigilancia u otras organizaciones similares (referidas como clientes ONVIF) a acceder a flujos de vídeo en directo y grabados desde el sistema XProtect VMS a las soluciones de monitorización central. Los flujos de vídeo se envían como transmisiones RTSP por Internet.

Las principales ventajas son:

[1]Disposición predefinida para uno o varios monitores Smart Wall en XProtect Smart Client. Los valores preestablecidos determinan qué cámaras se muestran y cómo se estructura el contenido en cada monitor del panel de vídeo.

- Habilita la interoperabilidad real y la libertad de elección para implementaciones de seguridad de múltiples proveedores a gran escala y una perfecta integración de video de privado a público
- Proporciona acceso externo a flujos de vídeo H.264 y H.265 en el sistema XProtect VMS, tanto vídeo en directo como reproducción
- Ofrece interfaces estandarizadas que proporcionan una forma sencilla y sin problemas de integrar soluciones de XProtect VMS con centros de alarmas y estaciones de monitorización

Este documento proporciona lo siguiente:

- Información sobre el estándar ONVIF y enlaces a materiales de referencia
- Instrucciones para instalar y configurar el Milestone Open Network Bridge en su producto XProtect VMS
- Ejemplos de cómo habilitar distintos tipos de clientes ONVIF para transmitir vídeo en directo y grabado desde productos de XProtect VMS

XProtect DLNA Server (explicación)

Este producto ya no es compatible con Milestone.

Milestone ha desarrollado productos add-on que se integran completamente XProtect para darle una funcionalidad extra. Su archivo de licencia de XProtect controla el acceso a productos add-on.

DLNA (Digital Living Network Alliance) es un estándar para conectar dispositivos multimedia. Los fabricantes de aparatos electrónicos obtienen la certificación DLNA de sus productos para garantizar la interoperabilidad entre distintos proveedores y dispositivos y habilitar así la distribución de contenidos de vídeo.

Las pantallas y televisores públicos suelen tener certificación DLNA y estar conectados a una red. Son capaces de escanear la red en busca de contenidos multimedia, conectarse al dispositivo y solicitar un flujo de medios a su reproductor multimedia integrado. XProtect DLNA Server puede ser descubierto por ciertos dispositivos con certificación DLNA y entregar secuencias de vídeo en directo desde cámaras seleccionadas a dispositivos con certificación DLNA con un reproductor multimedia.

Los dispositivos DLNA tienen un retardo de vídeo en directo de 1 a 10 segundos. Esto se debe a los diferentes tamaños de búfer de 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.

Dispositivos

Hardware (explicación)

El hardware representa o:

- 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
- Un servidor de grabación en un sitio remoto en una configuración Milestone Interconnect

Tiene varias opciones para añadir hardware a cada servidor de grabación de su sistema.

> ⚠ Si su hardware se encuentra detrás de un router con NAT o de un cortafuegos, es posible que tenga que especificar un número de puerto diferente y configurar el router/cortafuegos de forma que planifique el puerto y las direcciones IP que utiliza el hardware.

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

Preconfiguración de hardware (explicación)

Determinados fabricantes requieren establecer las credenciales en hardware listo para usarse de inmediato antes de añadir el hardware a un sistema VMS por primera vez. Esto se conoce como la preconfiguración de hardware y se hace mediante el asistente de **Preconfigurar dispositivos de hardware** que aparece cuando el asistente de Añadir hardware en la página 217 detecta dicho hardware.

Alguna información importante sobre el asistente **Preconfigurar dispositivos de hardware**:

- El hardware que requiere credenciales de inicio antes de ser añadido a un sistema VMS no se puede añadir utilizando las credenciales típicas predeterminadas y debe configurarse mediante el asistente o conectando con el hardware directamente
- Solo puede aplicar credenciales (nombre de usuario o contraseña) a campos marcados como **no establecido**
- Una vez que el **estado** del hardware se ha establecido en **configurado**, no puede cambiar las credenciales (nombre de usuario y contraseña)
- La configuración previa se aplica a hardware listo para usarse y solo se debe realizar una vez. Una vez preconfigurado, el hardware puede gestionarse como cualquier otro hardware en Management Client
- Después de cerrar el asistente **Preconfigurar dispositivos de hardware**, el hardware preconfigurado aparecerá en el asistente de Añadir hardware en la página 217, y ahora se puede aádir a su sistema

> ⚠ Es muy recomendable que añada el hardware preconfigurado en su sistema completando el asistente de Añadir hardware en la página 217 después de cerrar el asistente de **Preconfigurar dispositivos de hardware**. Management Client no retendrá las credenciales preconfiguradas si no añade el hardware a su sistema.

Devices (explicación)

El hardware tiene una serie de dispositivos que puede gestionar individualmente, por ejemplo:

- Una cámara física tiene dispositivos que representan la parte de la cámara (lentes), así como micrófonos, altavoces, metadatos, entrada y salida, ya sea adjuntos o integrados
- 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 los micrófonos, altavoces, metadatos, entrada y salida ya sea adjunta o integrada
- Un módulo de E/S tiene dispositivos que representan los canales de entrada y salida para, por ejemplo, las luces
- Un módulo de audio dedicado tiene dispositivos que representan las entradas y salidas de micrófonos y altavoces
- En una configuración Milestone Interconnect, el sistema remoto aparece como hardware con todos los dispositivos del sistema remoto en una lista

El sistema añade automáticamente los dispositivos del hardware cuando añade el hardware.

Para obtener información sobre el hardware compatible, consulte la página de hardware compatible en el sitio web Milestone (https://www.milestonesys.com/support/tools-and-references/supported-devices/).

Las siguientes secciones describen cada uno de los tipos de dispositivos que puede añadir.

Cámaras

Los dispositivos de la cámara envían flujos de vídeo al sistema que los usuarios clientes pueden utilizar para ver el vídeo en directo o que el sistema puede grabar para su posterior reproducción por parte de los usuarios clientes. Los cometidos determinan el permiso de los usuarios para ver el vídeo.

Micrófonos

En muchos dispositivos, puede conectar micrófonos externos. Algunos dispositivos tienen micrófonos integrados.

Los dispositivos con micrófono envían flujos de audio al sistema que los usuarios clientes pueden escuchar en directo o que el sistema puede grabar para su posterior reproducción por parte de los usuarios clientes. Puede configurar el sistema para recibir eventos específicos del micrófono que activen las acciones pertinentes.

Los cometidos determinan el permiso de los usuarios para escuchar a micrófonos. No puede escuchar a micrófonos desde el Management Client.

Altavoces

En muchos dispositivos se pueden conectar altavoces externos. Algunos dispositivos tienen altavoces integrados.

El sistema envía un flujo de audio a los altavoces cuando un usuario pulsa el botón de hablar en XProtect Smart Client. También puede usar esta función desde XProtect Web Client y XProtect® Mobile. El audio del altavoz solo se graba cuando le habla un usuario. Los cometidos determinan el permiso de los usuarios para hablar a través de los altavoces. No se puede hablar por los altavoces del Management Client.

Si dos usuarios quieren hablar al mismo tiempo, los cometidos determinan el permiso de los usuarios para hablar por los altavoces. Como parte de la definición de los cometidos, se puede especificar una prioridad del altavoz desde muy alta hasta muy baja. Si dos usuarios quieren hablar al mismo tiempo, el usuario cuyo cometido tiene la mayor prioridad gana la capacidad de hablar. Si dos usuarios con el mismo cometido quieren hablar al mismo tiempo, se aplica el principio del orden de llegada.

Metadatos

Los dispositivos de metadatos entregan al sistema flujos de datos que los usuarios clientes pueden utilizar para ver datos sobre los datos, por ejemplo, datos que describen la imagen de vídeo, el contenido o los objetos de la imagen, o la ubicación de donde se grabó la imagen. Los metadatos pueden ir unidos a cámaras, micrófonos o altavoces.

Los metadatos pueden ser generados por:

- El propio dispositivo que proporciona los datos, por ejemplo, una cámara que proporciona vídeo
- Un sistema de terceros o la integración mediante un controlador de metadatos genérico

Los metadatos generados por el dispositivo se vinculan automáticamente a uno o varios dispositivos del mismo hardware.

Los cometidos determinan el permiso de los usuarios para ver metadatos.

Entradas

En muchos dispositivos, puede conectar unidades externas a los puertos de entrada del dispositivo. Las unidades de entrada suelen ser sensores externos. Puede utilizar estos sensores externos, por ejemplo, para detectar si se abren puertas, ventanas o compuertas. Las entradas procedentes de estas unidades de entrada externas son tratadas por el sistema como eventos.

Puede utilizar estos eventos en reglas. Por ejemplo, puede crear una regla que especifique que una cámara debe empezar a grabar cuando se active una entrada y dejar de grabar 30 segundos después de que se desactive la entrada.

Salidas

En muchos dispositivos, puede conectar unidades externas a los puertos de salida del dispositivo. Esto le permite activar/desactivar luces, sirenas, etc. a través del sistema.

Puede utilizar la salida al crear reglas. Puede crear reglas que activen o desactiven automáticamente las salidas, y reglas que desencadenen acciones cuando se cambie el estado de una salida.

Device groups (explicación)

La agrupación de dispositivos en grupos de dispositivos forma parte del asistente para **Añadir hardware**, pero siempre se pueden modificar los grupos y añadir más grupos si es necesario.

Puede beneficiarse de la agrupación de diferentes tipos de dispositivos (cámaras, micrófonos, altavoces, metadatos, entradas y salidas) en su sistema:

- Los grupos de dispositivos le ayudan a mantener una visión general intuitiva de los dispositivos de su sistema
- Los dispositivos pueden existir en varios grupos
- Pueds crear subgrupos y subgrupos en subgrupos
- Puede especificar propiedades comunes para todos los dispositivos de un grupo de dispositivos de una sola vez
- Las propiedades de los dispositivos establecidas a través del grupo no se almacenan para el grupo sino en los dispositivos individuales
- Cuando se trata con cometidos, puede especificar la configuración de seguridad común para todos los dispositivos dentro de un grupo de dispositivos de una sola vez
- Cuando se trata con reglas, 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 necesite, pero no puede mezclar diferentes tipos de dispositivos (por ejemplo, cámaras y altavoces) en un grupo de dispositivos.

Cree grupos de dispositivos con **menos** de 400 dispositivos para poder ver y editar todas las propiedades.

Si elimina un grupo de dispositivos, solo eliminará el propio grupo de dispositivos. Si desea eliminar un dispositivo, por ejemplo una cámara, de su sistema, hágalo en el nivel del servidor de grabación.

Los siguientes ejemplos se basan en la agrupación de cámaras en grupos de dispositivos, pero los principios se aplican a todos los dispositivos

Añadir un grupo de dispositivos

Especificar qué dispositivos incluir en un grupo de dispositivos

Especificar propiedades comunes para todos los dispositivos de un grupo de dispositivos

Almacenamiento multimedia

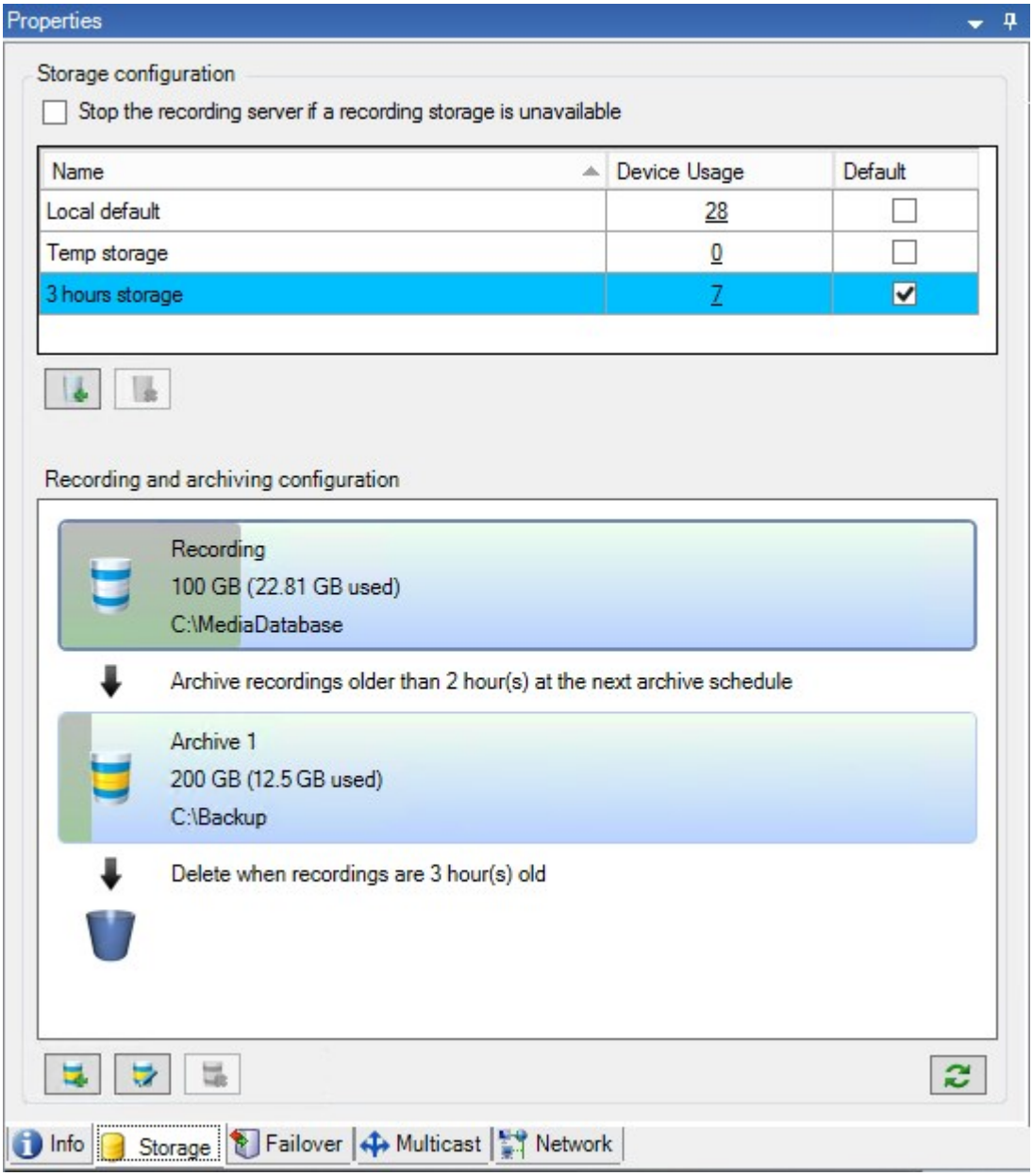
Almacenamiento y archivado (explicación)

La funcionalidad disponible depende del sistema que esté utilizando. Vea la lista completa de características, que está disponible en la página de descripción del producto en el sitio web Milestone (https://www.milestonesys.com/solutions/platform/product-index/).

En la pestaña **Almacenamiento**, puede configurar, gestionar y ver los almacenamientos de un servidor de grabación seleccionado.

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

Si está utilizando el **Bloqueo de evidencias**, habrá una línea roja vertical que mostrará el espacio utilizado para las secuencias bloqueadas de evidencias.



Cuando una cámara graba vídeo o audio, todas las grabaciones especificadas se almacenan, de forma predeterminada, en el almacenamiento definido para el dispositivo. Cada almacenamiento consta de un almacenamiento de grabaciones que guarda las grabaciones en la base de datos de grabaciones **Grabación**. Un almacenamiento no tiene archivo(s) predeterminado(s), pero puede crearlos.

Para evitar que la base de datos de grabaciones se llene, puede crear almacenamientos adicionales (consulte Añadir un nuevo almacenamiento en la página 202). También puede crear archivos (consulte Crear un archivo dentro de un almacenamiento en la página 203) en cada almacenamiento y empezar el proceso de archivado para almacenar datos.

El archivado es la transferencia automática de grabaciones desde, por ejemplo, la base de datos de grabaciones de una cámara a otra ubicación. De este modo, la cantidad de grabaciones que puede almacenar no se limita al tamaño de la base de datos de grabaciones. Con el archivado también puede hacer una copia de seguridad de sus grabaciones en otro soporte.

Configure el almacenamiento y el archivo en cada servidor de grabaciones.

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

Si un disco se rompe y el almacenamiento de grabaciones deja de estar disponible, la barra horizontal se pone de color rojo. Aún es posible ver vídeo en directo en XProtect Smart Client, pero la grabación y el archivado se detienen hasta que la unidad de disco se restablece. Si su sistema está configurado con servidores de grabación de failover, puede especificar que el servidor de grabaciones deje de funcionar, para que los servidores de failover asuman el control (consulte Especificar el comportamiento cuando el almacenamiento de la grabación no está disponible en la página 201).

Lo siguiente principalmente menciona cámaras y vídeo, pero también se aplica a altavoces, micrófonos, audio y sonido.

Milestone recomienda que utilice una unidad de disco duro dedicada para grabar almacenamientos y archivos para prevenir un rendimiento lento del disco. Al formatear el disco duro, es importante cambiar su ajuste **Tamaño de unidad de asignación** de 4 a 64 kilobytes. Esto no mejora significativamente el rendimiento de la grabación del disco duro. Puede leer más sobre tamaños de unidades de asignación y encontrar ayuda en el sitio web de Microsoft (https://support.microsoft.com/en-us/topic/default-cluster-size-for-ntfs-fat-and-exfat-9772e6f1-e31a-00d7-e18f-73169155af95).

Los datos más antiguos de una base de datos siempre se archivan de forma automática (o se eliminan si no se ha definido el siguiente archivo) cuando quedan menos de 5 GB de espacio libre. Si hay menos de 1 GB de espacio libre, los datos se eliminan. Una base de datos siempre requiere 250 MB de espacio libre. Si alcanza este límite porque los datos no se eliminan lo bastante rápido, los intentos de escribir en la base de datos podrían fallar y, en ese caso, no se escriben más datos en la base de datos hasta que libere espacio suficiente. El tamaño máximo real de su base de datos pasa a ser la cantidad de gigabytes que especifique, menos 5 GB.

En el caso de los sistemas que cumplan con FIPS 140-2, con exportaciones y bases de datos de medios archivados de versiones de XProtect VMS anteriores a 2017 R1 que estén cifrados con cifrados que no cumplan con FIPS, es necesario archivar los datos en una ubicación en la que se pueda seguir accediendo a ellos después de habilitar FIPS. Para obtener información detallada sobre cómo configurar su XProtect VMS para que se ejecute en modo compatible con FIPS 140-2, consulte la sección de cumplimiento de FIPS 140-2 la guía de endurecimiento.

Adjuntar dispositivos a un almacenamiento

Una vez configurados los ajustes de almacenamiento y archivo para un servidor de grabaciones, puede habilitar el almacenamiento y el archivo para cámaras individuales o para un grupo de cámaras. Lo hace desde los dispositivos individuales o desde el grupo de dispositivos. Consulte Adjuntar un dispositivo o grupo de dispositivos a un almacenamiento en la página 203.

Archivado efectivo

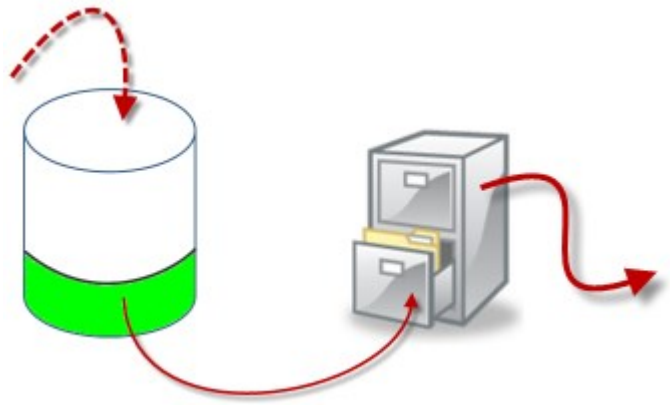
Al habilitar el archivado para una cámara o un grupo de cámaras, el contenido del almacenamiento de grabaciones se mueve automáticamente al primer archivo a intervalos que usted defina.

Dependiendo de sus requisitos, puede configurar uno o más archivos para cada uno de sus almacenamientos. Los archivos pueden estar ubicados en el propio ordenador del servidor de grabaciones o en otra ubicación a la que tenga accesoel sistema, por ejemplo una unidad de red.

AL configurar su archivado de una manera efectiva, puede optimizar las necesidades de almacenamiento. A menudo, se desea que las grabaciones archivadas ocupen el menor espacio posible, sobre todo a largo plazo, donde tal vez sea posible incluso aflojar un poco la calidad de la imagen. Maneje el archivado efectivo desde la pestaña **Almacenamiento** de un servidor de grabaciones ajustando varos ajustes interdependientes:

- Retención del almacenamiento de grabaciones
- Tamaño del almacenamiento de grabaciones
- Retención del archivo
- Tamaño del archivo
- Calendario de archivo
- Cifrado
- Fotogramas por segundo (FPS).

Los campos de tamaño definen el tamaño del almacenamiento de grabaciones, ejemplificado en el cilindro y su(s) archivos(s) respectivamente:



Por medio del ajuste del tiempo de retención y el tamaño para el almacenamiento de grabaciones, ejemplificado por la zona blanca del cilindro, se define la antigüedad que deben tener las grabaciones antes de que se archiven. En nuestro ejemplo ilustrado, archiva las grabaciones cuando son lo bastante antiguas para archivarlas.

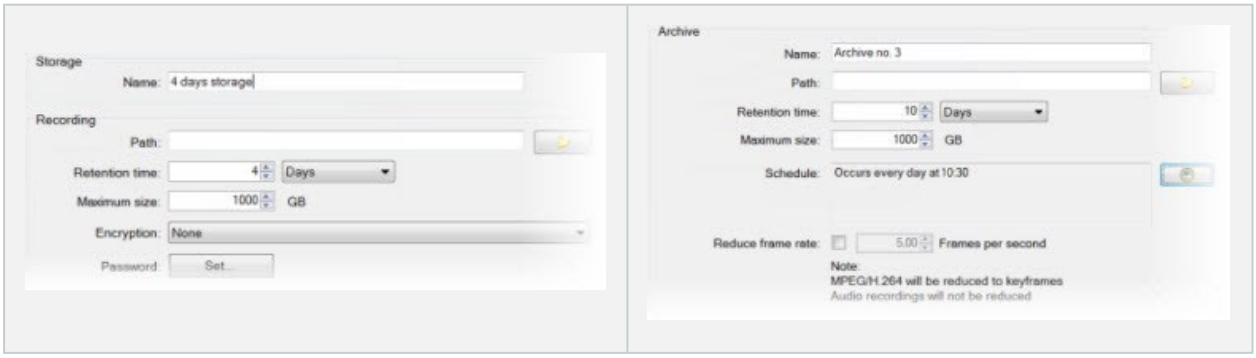
El ajuste de tiempo de retención y tamaño para archivos define el tiempo que permanecen las grabaciones en el archivo. Las grabaciones permanecen en el archivo durante el tiempo especificado o hasta que el archivo haya alcanzado el límite de tamaño especificado. Cuando se cumplen estos ajustes, el sistema empieza a sobrescribir grabaciones antiguas en el archivo.

El calendario de archivado define con qué frecuencia y en qué momentos tiene lugar el archivado.

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

Para archivar sus grabaciones, debe establecer todos estos parámetros unos de acuerdo con otros. Eso significa que el periodo de retención del siguiente archivo siempre debe ser más largo que el periodo de retención de una base de datos de grabaciones o un archivo actuales. Esto se debe al número de días de retención indicados para un archivo incluye toda la retención indicada previamente en el proceso. El archivado también debe tener lugar siempre con más frecuencia que el periodo de retención, de lo contrario se arriesga a perder datos. Si tiene un tiempo de retención de 24 horas, cualquier dato con una antigüedad superior a 24 horas se elimina. Por lo tanto, para conseguir que sus datos se muevan de forma segura al siguiente archivo, es importante realizar el archivado con más frecuencia que cada 24 horas.

Ejemplo: Estos almacenamientos (imagen de la izquierda) tienen un tiempo de retención de 4 dñias y el siguiente archivo (imagen de la derecha) tiene un tiempo de retención de 10 días. El archivado está establecido para que se produzca todos los días a las 10:30, lo que garantiza un archivado mucho más frecuente que el tiempo de retención.



También puede controlar el archivado utilizando reglas y eventos.

Estructura del archivo (explicación)

Al archivar grabaciones, se almacenan en una determinada estructura de subdirectorios dentro del archivo.

> Durante todo el uso regular de su sistema, la estructura de subdirectorios es completamente transparente para los usuarios del sistema, ya que examinan todas las grabaciones con el XProtect Smart Client con independencia de si las grabaciones están o no archivadas. Conocer la estructura de los subdirectorios es principalmente interesante si quiere hacer una copia de seguridad de sus grabaciones archivadas.

En cada uno de los directorios de archivos del servidor de grabaciones, el sistema crea automáticamente subdirectorios separados. Estos subdirectorios tienen el nombre del dispositivo y la base de datos de archivos.

Debido a que puede almacenar grabaciones de distintas cámaras en el mismo archivo, y dado que el archivado para cada cámara es probable que se produzca a intervalos regulares, también se añaden otros subdirectorios automáticamente.

Estos subdirectorios representan, cada uno, aproximadamente el equivalente a una hora de grabaciones. La división de una hora hace que sea posible quitar solo partes relativamente pequeñas de los datos de un archivo si alcanza el tamaño máximo permitido del archivo.

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

Estructura de la nomenclatura

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

Si el desde el almacenamiento periférico:

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

Si es desde SMTP:

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

Ejemplo de la vida real

```
...F:\OurArchive\Archive1\Camera 1 en Axis Q7404 Codificador de vídeo
(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 subdirectorios dependen de la naturaleza de las grabaciones reales. Por ejemplo, varios subdirectorios distintos se añaden si las grabaciones se dividen técnicamente en secuencias. Este es a menudo el caso si ha usado la detección de movimiento para desencadenar grabaciones.

- **Medios**: Esta carpeta contiene el medio real que es vídeo o audio (no ambos)
- **MotionLevel**: Esta carpeta contiene cuadrículas de nivel de movimiento generada a partir de los datos de vídeo utilizando nuestro algoritmo de detección de movimiento. Estos datos permiten que la característica Búsqueda inteligente en XProtect Smart Client haga búsquedas muy rápidas
- **Movimiento**: En esta carpeta, el sistema almacena secuencias de movimiento. Una secuencia de movimiento es un periodo de tiempo para el que se ha detectado movimiento en los datos del vídeo. Esta información, por ejemplo, se usa en la misma línea de tiempo en XProtect Smart Client
- **Grabación**: En esta carpeta, el sistema almacena secuencias de grabación. Una secuencia de grabación es un periodo de tiempo para el que existen grabaciones coherentes de datos de medios. Esta información, por ejemplo, se usan para trazar la línea de tiempo en XProtect Smart Client
- **Firma**: Esta carpeta contiene las firmas generadas para los datos del medio (en la carpeta Medios). Con esta información, puede verificar que los datos de medios no se han alterado desde su grabación

Si quiere hacer una copia de seguridad de sus archivos, puede orientar sus copias de seguridad si conoce los aspectos básicos de la estructura de subdirectorios.

Ejemplos de copia de seguridad

Para hacer una copia de seguridad del contenido de un archivo entero, haga la copia de seguridad del directorio del archivo requerido y de todo su contenido. Por ejemplo, todo en:

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

Para hacer una copia de seguridad de las grabaciones de una cámara concreta de un periodo de tiempo concreto, haga la copia de seguridad únicamente del contenido de los subdirectorios relevantes. Por ejemplo, todo en:

```
...F:\OurArchive\Archive1\Camera 1 en Axis Q7404 Codificador de vídeo
(10.100.50.137) - 2011-10-05T11:23:47+02:00\
```

Almacenamiento previo en búfer y almacenamiento de grabaciones (explicación)

El almacenamiento previo en búfer es la capacidad de grabar audio y vídeo antes de que se produzca el evento de activación real. Esto es útil cuando se quiere grabar el audio o el vídeo que conduce a un evento que activa la grabación, por ejemplo, la apertura de una puerta.

El almacenamiento previo en búfer es posible porque el sistema recibe continuamente flujos de audio y vídeo de los dispositivos conectados y los almacena temporalmente durante el periodo de almacenamiento previo en búfer definido.

- Si se activa una regla de grabación, las grabaciones temporales se convierten en permanentes durante el tiempo de pregrabación configurado por la regla
- Si no se activa ninguna regla de grabación, las grabaciones temporales en el pre-buffer se borran automáticamente después del tiempo de pre-buffer definido

Almacenamiento de las grabaciones temporales del búfer previo

Puede elegir el lugar de almacenamiento de las grabaciones temporales del pre-buffer:

- En la memoria; el periodo de pre-buffer está limitado a 15 segundos.
- En el disco (en la base de datos de medios); puede elegir todos los valores.

El almacenamiento en la memoria, en lugar de en el disco, mejora el rendimiento del sistema, pero solo es posible para periodos más cortos de pre-buffer.

Cuando las grabaciones se almacenan en la memoria, y hace que algunas de las grabaciones temporales sean permanentes, las grabaciones temporales restantes se borran y no se pueden restaurar. Cuando las grabaciones se almacenan en la memoria, y hace que algunas de las grabaciones temporales sean permanentes, las grabaciones temporales restantes se borran y no se pueden restaurar. Si necesita poder conservar las grabaciones restantes, almacene las grabaciones en el disco.

Autenticación

Active Directory (explicación)

Active Directory es un servicio de directorios distribuido implementado por Microsoft para redes de dominio de Windows. Está incluido en la mayoría de sistemas operativos de Windows Server. Identifica recursos en una red para que los usuarios o las aplicaciones accedan a ellos.

Con Active Directory instalado, puede añadir usuarios de Windows de Active Directory, pero también tiene la opción de añadir usuarios básicos sin Active Directory. Existen ciertas limitaciones del sistema relacionadas con usuarios básicos.

Usuarios (explicación)

El término **usuarios** se refiere principalmente a usuarios que se conectan al sistema de vigilancia a través de clientes. Puede configurar estos usuarios de dos formas:

- Como **usuarios básicos**, la autenticación se realiza mediante una combinación de nombre de usuario y contraseña
- Como **usuarios de Windows** la autenticación se basa en su inicio de sesión en Windows

Usuarios de Windows

Añade usuarios de Windows mediante el uso de Active Directory. Active Directory (AD) es un servicio de directorios implementado por Microsoft para redes de dominios de Windows. Está incluido en la mayoría de sistemas operativos de Windows Server. Identifica recursos en una red para que los usuarios o las aplicaciones accedan a ellos. Active Directory utiliza los conceptos de usuarios y grupos.

Los usuarios son objetos de Active Directory que representan a individuos 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. Al añadir un grupo al sistema, se añade a todos sus miembros de una vez. Una vez añadido el grupo al sistema, cualquier cambio realizado en el grupo en Active Directory, como añadir nuevos miembros o quitar miembros antiguos en una fase posterior, se ven reflejados de inmediato en el sistema. Un usuario puede ser miembro de varios grupos a la vez.

Puede utilizar Active Directory para añadir información de usuarios y grupos existentes al sistema con algunas ventajas:

- Los usuarios y los grupos se especifican centralmente en Active Directory para que no tenga que crear cuentas de usuario desde cero
- No tiene que configurar ninguna autenticación de usuarios en el sistema, ya que Active Directory maneja la autenticación

Antes de poder añadir usuarios y grupos mediante el 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. Para obtener información sobre cómo configurar usuarios básicos, consulte Crear usuarios básicos en la página 297.

Identity Provider (explicación)

Identity Provider app pool (IDP) es una entidad del sistema que crea, mantiene y gestiona información de identidad para usuarios básicos.

Identity Provider también proporciona servicios de autenticación y registro a las aplicaciones o los servicios dependientes, en este caso: Servidor de grabaciones, Servidor de gestión, Data Collector y Servidor de informes.

Cuando inicie sesión en clientes y servicios de XProtect como usuario básico, su solicitud va al Identity Provider. Una vez autenticado, el usuario puede llamar al servidor de gestión.

Identity Provider ejecuta el IIS como parte del servidor de gestión utilizando el mismo SQL Server con una base de datos independiente y es responsable de crear y manejar los tokens de comunicación de OAuth que presta servicio al uso cuando se comunica (Surveillance_IDP).

Identity Provider los registros se pueden encontrar en \\Datos de programa\Milestone\IDP\Registros.

IDP externo (explicación)

IDP es un acrónimo para Identity Provider. Un IDP externo es una aplicación y un servicio externo donde puede almacenar y gestionar la información de la identidad del usuario y proporcionar servicios de autenticación de usuarios a otros sistemas. Puede asociar un IDP externo con el VMS de XProtect.

XProtect VMS admite IDP externos compatibles con OpenID Connect (OIDC).

Reclamaciones (explicación)

Las reclamaciones constituyen el vínculo entre el IDP externo y el VMS de XProtect.

Una reclamación es una declaración que una entidad, como un usuario o una aplicación, hace sobre sí misma. En el VMS de XProtect, una reclamación puede estar asociada a unos cometidos que determinan los permisos de los usuarios de XProtect.

La reclamación es un valor clave que consiste en un nombre de reclamación y un valor de reclamación. Por ejemplo, el nombre de la reclamación podría ser un nombre estándar que describa el contenido del valor de la reclamación, y el valor de la reclamación podría ser el nombre de un grupo. Vea más ejemplos de reclamaciones de un IDP externo: Ejemplo de reclamaciones de un IDP externo.

Habilitar a los usuarios para iniciar sesión en el VMS de XProtect desde un IDP externo

- Desde el IDP externo, cree los usuarios. También debe identificar el VMS de XProtect y la interacción entre XProtect y el IDP externo. Finalmente, cree las reclamaciones para identificar usuarios como usuarios de IDP externo en el VMS de XProtect.
- Desde el VMS de XProtect, cree una configuración que habilite al Identity Provider a contactar con el IDP externo. Para obtener más información sobre cómo crear una configuración para un IDP externo, consulte Añadir y configurar un IDP externo.
- Desde el VMS de XProtect, establezca la autenticación de los usuarios asignando las reclamaciones de los usuarios desde el IDP externo a los cometidos de XProtect. Para obtener más información sobre cómo asignar reclamaciones a los cometidos, consulte Asignar reclamaciones desde un IDP externo a cometidos en XProtect.

Redirigir URI

Redirigir URI especifica la página a la que se envía al usuario tras una autenticación exitosa. En su IDP externo, debe añadir la dirección del servidor de gestión y a continuación la **ruta de devolución de llamada** que definió en XProtect Management Client. Por ejemplo, https://management-server-computer.company.com/idp/signin-oidc

Nombres de usuario únicos para usuarios de IDP externos

Los nombres de usuario se crean automáticamente para los usuarios que inician sesión en Milestone XProtect a través de un IDP externo.

El IDP externo proporciona un conjunto de reclamaciones para crear automáticamente un nombre para el usuario en XProtect, y en XProtect un algoritmo se utiliza para elegir un nombre del IDP externo que es único en la base de datos VMS.

Ejemplo de reclamaciones de un IDP externo

Las reclamaciones constan de un nombre de reclamación y un valor de reclamación. Por ejemplo:

Nombre de la reclamación	Valor de la reclamación
nombre	Raz Van
correo electrónico	123@dominio.com
amr	pwd
idp	00o2ghkgazGgi9BIE5d7
preferred_ username	321@dominio.com
vmsRole	Operador
locale	en-US
given_name	Raz
family_name	Lindberg
zoneinfo	America/Los_Angeles
email_verified	Verdadero

Utilizar el número de secuencia de la demanda para crear nombres de usuario en XProtect

En XProtect, la prioridad de búsqueda para cuando se crea un usuario en el VMS de XProtect está controlada por el número de secuencia de las reclamaciones en la tabla siguiente. Se utilizará el primer nombre de reclamación disponible en el VMS de XProtect:

Nombre de la reclamación	Número de secuencia	Descripción
UserNameClaimType	1	Asignación configurada con una reclamación

Nombre de la reclamación	Número de secuencia	Descripción
		para definir el nombre del usuario. La reclamación se define en el campo **Reclamación para utilizar para crear el nombre de usuario** en la pestaña **IDP externo** en **Herramientas** > **Opciones**.
preferred_username	2	Reclamación que puede provenir del IDP externo. Una reclamación estándar que normalmente se utiliza para esto en Oidc (OpenID Connect).
nombre	3	
given_name family_ name	4	Nombre y apellido en una combinación como Bob Johnson.
correo electrónico	5	
Primera reclamación disponible + #(primer número disponible)	6	Por ejemplo, Bob#1

Definir reclamaciones específicas para crear nombres de usuario en XProtect

Los administradores de XProtect pueden definir una reclamación específica desde el IDP externo que se debe utilizar para crear un nombre de usuario en el VMS de XProtect. Cuando un administrador define una reclamación para utilizarla para la creación del nombre de usuario en el VMS de XProtect, el nombre de la reclamación debe escribirse exactamente como el nombre de la reclamación procedente del IDP externo.

- La reclamación para utilizar el nombre de usuario puede definirse en el campo **Reclamación para utilizar para crear el nombre de usuario** en la pestaña **IDP externo** en **Herramientas** > **Opciones** .

Eliminación de usuarios de IDP externos

Los usuarios creados en XProtect por un inicio de sesión de IDP externo se eliminan de la misma manera que un usuario básico y el usuario puede ser eliminado en cualquier momento después de la creación del usuario.

Si se elimina un usuario en XProtect y el usuario inicia sesión de nuevo desde el IDP externo, se creará un nuevo usuario en XProtect. Sin embargo, los datos asociados al usuario en XProtect como las vistas privadas y los cometidos se pierden y hay que crear de nuevo esta información para el usuario en XProtect.

Si se elimina un IDP externo en el Management Client, todos los usuarios conectados al VMS mediante el IDP externo también se eliminan.

Seguridad

Cometidos y permisos de un cometidos (explicación)

Todos los usuarios en Milestone XProtect VMS pertenecen a un cometido.

Los cometidos determinan los permisos de los usuarios, incluidos los dispositivos a los que pueden acceder. Los cometidos también determinan la seguridad y los permisos de acceso dentro del sistema de gestión de vídeo.

El sistema cuenta con un cometido predeterminado de **Administrator** con acceso completo a todas las funcionalidades del sistema, pero en la mayoría de los casos se necesita más de un cometido en el sistema, para diferenciar entre usuarios y el acceso que deberían tener. Puede añadir tantos cometidos como desee. Consulte Asignar/eliminar usuarios y grupos a/de roles en la página 296.

Por ejemplo, es posible que necesite configurar distintos tipos de cometidos para los usuarios de XProtect Smart Client, en función de los dispositivos a los que desee que tengan acceso, o tipos de restricciones similares que requieran una diferenciación entre usuarios.

Para crear una diferenciación entre usuarios, deberá:

- Crear y configurar los cometidos que necesite para adaptarse a las necesidades empresariales de su organización.
- Añadir usuarios y grupos de usuarios que asigne a los cometidos a los que deben pertenecer.
- Crear perfiles de Smart Client y perfiles de Management Client para determinar lo que los usuarios pueden ver en la interfaz de usuario de XProtect Smart Client y Management Client.

  Los cometidos únicamente controlan sus permisos de acceso, y no lo que los usuarios pueden ver en la interfaz de usuario en XProtect Smart Client o el Management Client. No es necesario que cree un perfil específico Management Client para usuarios que nunca utilizarán el Management Client.

Para la mejor experiencia de usuario posible para usuarios de XProtect Smart Client o usuarios de Management Client con acceso limitado a la funcionalidad de Management Client, deberá asegurarse de que existe coherencia entre los permisos proporcionados por el cometido y los elementos de la interfaz de usuario proporcionados por el perfil Smart Client o Management Client.

> ⚠ Para tener acceso a Management Server, es importante que todos los cometidos tengan el permiso de seguridad **Conectar** habilitado. El permiso se encuentra en **Ajustes de cometidos** > **Management Server** > Pestaña Seguridad global (roles) en la página 540.

Para configurar roles en su sistema, expanda **Seguridad** > **Roles**.

Permisos de un cometido

La funcionalidad disponible depende del sistema que esté utilizando. Vea la lista completa de características, que está disponible en la página de descripción del producto en el sitio web Milestone (https://www.milestonesys.com/solutions/platform/product-index/).

Al crearse un cometido en el sistema, se puede asignar a dicho cometido una serie de permisos sobre los componentes o características del sistema a los que el cometido en cuestión puede acceder y utilizar.

Por ejemplo, es posible que desee crear cometidos que solo tengan permisos para acceder a la funcionalidad en XProtect Smart Client u otros clientes de visualización de Milestone con los permisos para ver solo ciertas cámaras. Si crea estos cometidos, estos cometidos no deberían tener permisos para acceder y utilizar el Management Client, sino solo tener acceso a algunas o todas las funcionalidades que se encuentran en XProtect Smart Client u otros clientes.

Para hacer frente a esta necesidad de diferenciación, deberá configurar seguidamente un cometido que tenga algunos o la mayoría de los permisos típicos de administrador, por ejemplo, los permisos para añadir y eliminar cámaras, servidores y funciones similares. Puede crear cometidos que tengan algunos o la mayoría de los permisos de un administrador del sistema. Esto puede, por ejemplo, ser relevante si su organización quiere separar entre personas que pueden administrar un subconjunto del sistema y personas que pueden administrar el sistema entero.

Los cometidos le dan la posibilidad de proporcionar permisos de administrador diferenciados para acceder, editar o cambiar una gran variedad de funciones del sistema. Por ejemplo, el permiso para editar la configuración de los servidores o cámaras de su sistema. Especifique estos permisos en la pestaña **Seguridad general** (consulte Pestaña Seguridad global (roles) en la página 540). Para habilitar que el administrador del sistema diferenciado pueda lanzar el Management Client, deberá conceder permisos de lectura en el servidor de gestión para este cometido.

> ⚠ Para tener acceso a Management Server, es importante que todos los cometidos tengan el permiso de seguridad **Conectar** habilitado. El permiso se encuentra en **Ajustes de cometidos** > **Management Server** > Pestaña Seguridad global (roles) en la página 540.

También puede reflejar las mismas limitaciones en la interfaz de usuario de Management Client para cada rol asociando el rol a un perfil de Management Client que tenga eliminadas de la interfaz de usuario las funciones del sistema correspondientes. Consulte Perfiles Management Client (explicación) en la página 73 para obtener información.

Para otorgar a un cometido estos permisos de administrador diferenciados, la persona con el cometido de administrador completo por defecto debe configurar el cometido en **Seguridad** > **Cometidos > Pestaña Información > Añadir nuevo**. Al configurar el nuevo rol, puede asociar el rol a sus propios perfiles de forma similar a cuando configura cualquier otro rol en el sistema o utiliza los perfiles predeterminados del sistema. Si desea más información, consulte Añadir y gestionar un rol en la página 295.

Cuando haya especificado los perfiles a los que quiere asociar el cometido, vaya a la pestaña **Seguridad general** para especificar los permisos del cometido.

Los permisos que puede establecer para un cometido son diferentes entre sus productos. Solo puede dar todos los permisos disponibles a un cometidos en XProtect Corporate.

Máscara de privacidad (explicación)

Máscara de privacidad (explicación)

Con la máscara de privacidad, puede definir qué áreas del vídeo de una cámara desea cubrir con máscaras de privacidad cuando se muestren en los clientes. Por ejemplo, si una cámara de vigilancia cubre una calle, puede cubrir ciertas zonas de un edificio (podrían ser ventanas y puertas) con máscaras de privacidad, para proteger la intimidad de los residentes. En algunos países, esto es un requisito legal.

Puede especificar las máscaras de privacidad como sólidas o borrosas. Las máscaras cubren tanto el vídeo en directo como el grabado y el exportado.

Las máscaras de privacidad se aplican y se bloquean en una zona de la imagen de la cámara, por lo que la zona cubierta no sigue los movimientos de paneo y zoom, sino que cubre constantemente la misma zona de la imagen de la cámara. En algunas cámaras PTZ, puede habilitar el enmascaramiento de privacidad basado en la posición en la propia cámara.

Hay dos tipos de máscaras de privacidad:

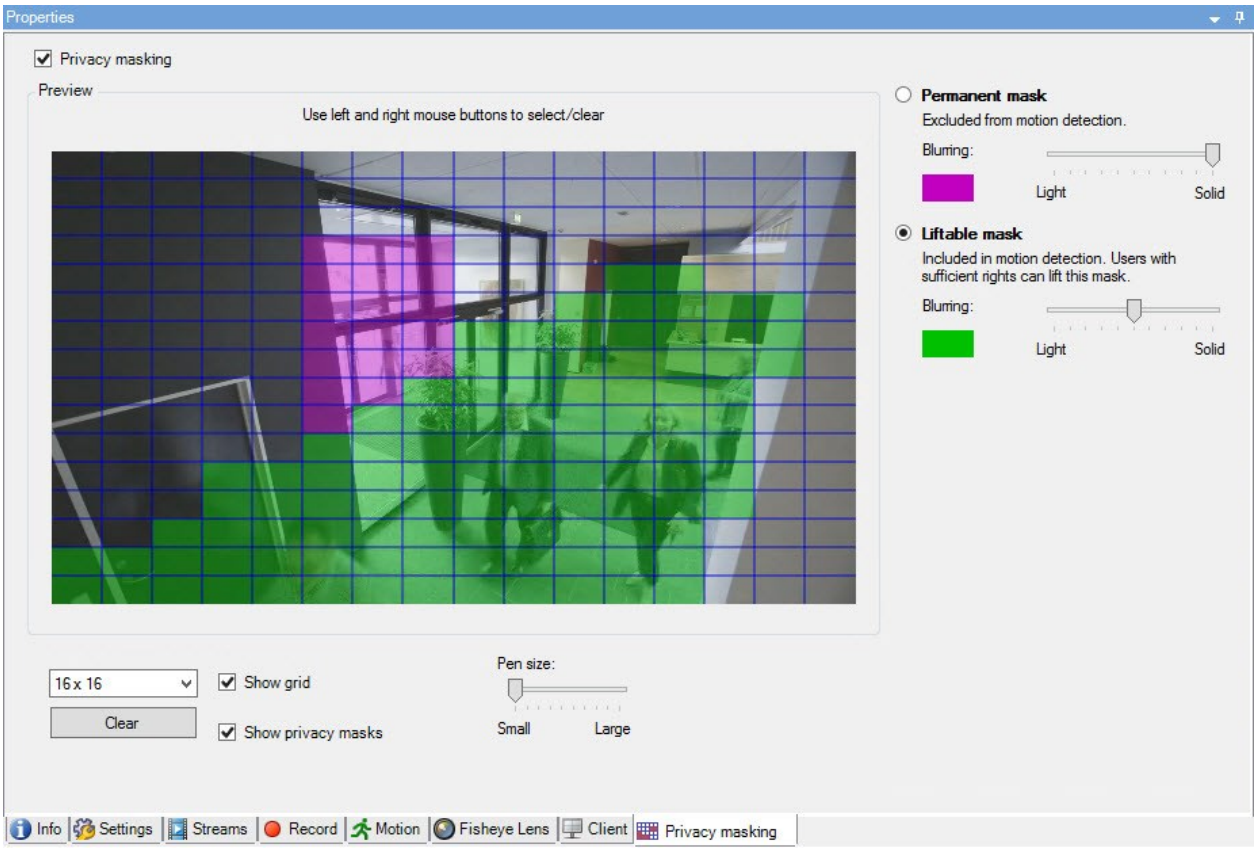
- **Máscara de privacidad permanente**: Las zonas con este tipo de máscara están siempre cubiertas en los clientes. Puede utilizarse para cubrir zonas del vídeo que nunca requieren vigilancia, como las zonas públicas o las zonas en las que no se permite la vigilancia. La detección de movimiento está excluida de las zonas con máscaras de privacidad permanentes
- **Máscara de privacidad elevable**: Las zonas con este tipo de máscara pueden ser descubiertas temporalmente en XProtect Smart Client por los usuarios con permiso para levantar las máscaras de privacidad. Si el usuario que ha iniciado la sesión en XProtect Smart Client no tiene permiso para levantar las máscaras de privacidad, el sistema solicita que un usuario autorizado apruebe el levantamiento.
  Las máscaras de privacidad se mantienen hasta que se agote el tiempo o el usuario las vuelve a aplicar. Tenga en cuenta que las máscaras de privacidad se levantan en el vídeo de todas las cámaras a las que el usuario tiene acceso

Si se actualiza desde un sistema 2017 R3 o anterior con máscaras de privacidad aplicadas, las máscaras se convertirán en máscaras elevables.

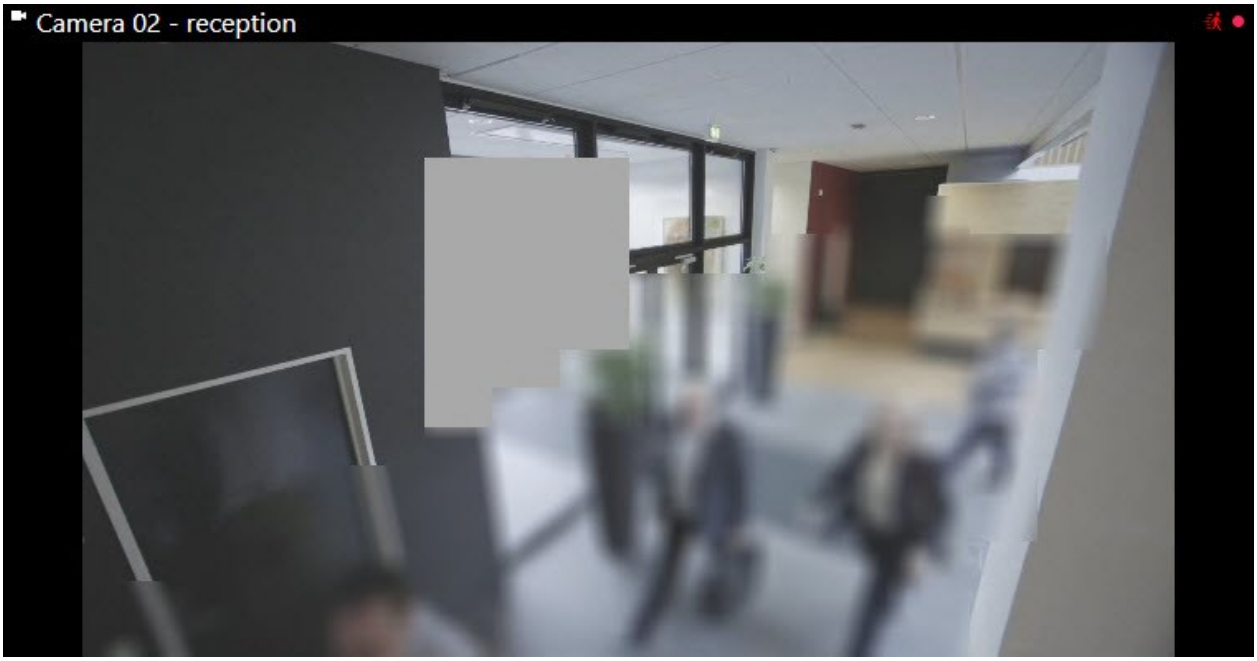
Cuando un usuario exporta o reproduce un vídeo grabado desde un cliente, el vídeo incluye las máscaras de privacidad configuradas en el momento de la grabación, incluso si ha cambiado o eliminado las máscaras de privacidad posteriormente. Si se levanta la proteción de seguridad al exportar, el vídeo exportado **no** incluye las máscaras de privacidad levantables.

Si cambia los ajustes de enmascaramiento de la privacidad con mucha frecuencia, por ejemplo, una vez a la semana, el sistema puede potencialmente sobrecargarse.

Ejemplo de la pestaña **Enmascaramiento de la privacidad** con máscaras de privacidad configuradas:



Y así es como aparecen en los clientes:



Puede informar a los usuarios clientes de los ajustes de las máscaras de privacidad permanentes y levantables.

Perfiles Management Client (explicación)

Management Client los perfiles permiten a los administradores del sistema modificar la interfaz de usuario de Management Client para otros usuarios. Asocie perfiles Management Client con los cometidos para limitar la interfaz de usuario para representar la funcionalidad disponible para cada cometido de administrador.

Management Client los perfiles solo manejan la representación visual de la funcionalidad del sistema, no el acceso real a ella. El acceso general a la funcionalidad del sistema se concede a través del cometido al que están asociados los usuarios individuales. Para obtener información sobre cómo gestionar el acceso general a la funcionalidad del sistema para un cometido, consulte Gestionar la visibilidad de la funcionalidad para un perfil Management Client.

Puede cambiar la configuración de la visibilidad de todos los elementos Management Client. Por defecto, el perfil Management Client puede ver todas las funcionalidades en el Management Client.

Smart Client perfiles (explicación)

La funcionalidad disponible depende del sistema que esté utilizando. Vea la lista completa de características, que está disponible en la página de descripción del producto en el sitio web Milestone (https://www.milestonesys.com/solutions/platform/product-index/).

Todos los usuarios en Milestone XProtect VMS pertenecen a un cometido al cual está conectado el perfil de Smart Client.

Los cometidos definen los permisos de los usuarios y los perfiles de Smart Client definen lo que los usuarios pueden ver en la interfaz de usuario de XProtect Smart Client.

Todas las instalaciones de Milestone XProtect VMS incluyen un **perfil predeterminado de cliente inteligente** que se ajusta con una configuración predeterminada para visualizar la mayor parte de los ajustes disponibles en el sistema de su organización. Algunos ajustes están siempre deshabilitados por defecto.

En los casos en los que tenga varios cometidos diferentes en una organización, es posible que desee desactivar la funcionalidad a la que un cometido en particular no tiene/no debería tener acceso en XProtect Smart Client.

Por ejemplo, puede tener una función cuyo trabajo diario no requiera ejecutar ninguna reproducción de vídeo. Para tal fin, puede crear un nuevo perfil de Smart Client para ese cometido en el que deshabilite el modo **Reproducción**. Al deshabilitar este ajuste en el perfil de Smart Client, los usuarios de XProtect Smart Client con un cometido que utilice este perfil de Smart Client ya no pueden ver el modo **Reproducción** en sus interfaces de usuario de XProtect Smart Client.

Es importante tener en cuenta que los perfiles de Smart Client controlan principalmente lo que los usuarios pueden ver en la interfaz de usuario de XProtect Smart Client y no los verdaderos permisos de acceso del cometido. Esos permisos de acceso, como el acceso a la lectura, modificación o eliminación, se controlan en las configuraciones del cometido. De este modo, los usuarios de XProtect Smart Client pueden disponer de permisos para funcionalidades a través de su cometido que no pueden ver en la interfaz de usuario porque está deshabilitado en el perfil de Smart Client.

Para que los usuarios de XProtect Smart Client disfruten de la mejor experiencia posible, debe asegurarse de que existe coherencia entre los permisos proporcionados por el cometido y los elementos de la interfaz de usuario proporcionados por el perfil de Smart Client.

Para crear o editar Smart Client perfiles, expanda **Cliente** y seleccione **Smart Client Perfiles**.

También puedes conocer la relación entre los perfiles Smart Client, los roles y los perfiles temporales y cómo utilizarlos conjuntamente (ver Crear y configurar perfiles, cometidos y perfiles temporales Smart Client en la página 270).

Bloqueos de evidencias (explicación)

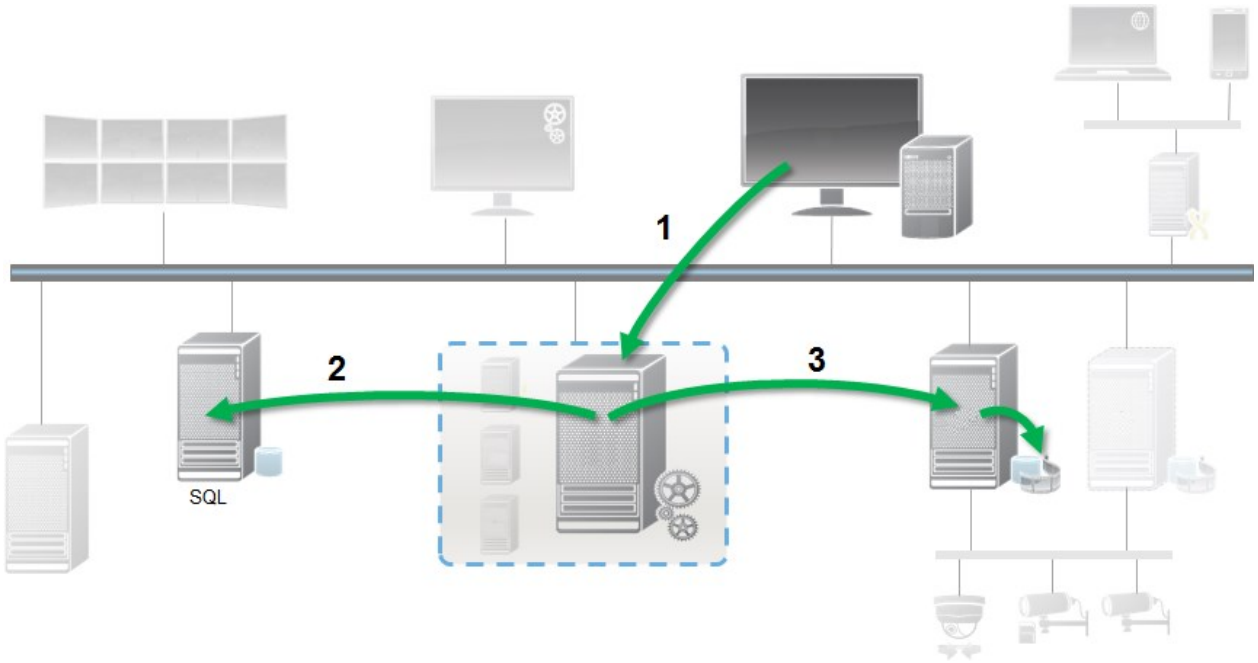
La funcionalidad disponible depende del sistema que esté utilizando. Vea la lista completa de características, que está disponible en la página de descripción del producto en el sitio web Milestone (https://www.milestonesys.com/solutions/platform/product-index/).

A partir deXProtect VMS, versión 2020 R2, cuando se actualiza el servidor de gestión de una versión anterior, no será posible crear ni modificar bloqueos de evidencias en servidores de grabación que sean de la versión 2020 R1 o anterior, hasta que estos servidores de grabación se hayan actualizado.
Esto también significa que, si el hardware se ha movido de un servidor de grabaciones (desde 2020 R1 o anterior) a otro servidor de grabación, y aún contiene grabaciones, loe bloqueos de evidencias no se pueden crear ni modificar.

Con la funcionalidad de bloqueo de evidencias, los operadores clientes pueden proteger secuencias de vídeo, incluido audio y otros datos, frente a su eliminación en caso necesario, por ejemplo, mientras hay una investigación o un ensayo en curso. Si desea más información, consulte el manual del usuario para XProtect Smart Client.

Cuando están protegidos, los datos no pueden eliminarse, ni automáticamente por el sistema después del tiempo de retención del sistema o en otras situaciones ni manualmente por los usuarios clientes. El sistema o un usuario no puede eliminar los datos hasta que un usuario con suficientes permisos desbloquee la evidencia.

Diagrama de flujo para Bloqueo de evidencias:



1. Un usuario de XProtect Smart Client crea un bloqueo de evidencias. Información enviada al Servidor de gestión.
2. El Servidor de gestión almacena información sobre el bloqueo de evidencias en la base de datos SQL.
3. El Servidor de gestión informa al Servidor de grabaciones de que almacene y proteja las grabaciones protegidas en la base de datos.

Cuando el operador crea un bloqueo de evidencias, los datos protegidos permanecen en el almacenamiento de grabaciones en el que se grabó, y se mueve a discos de archivado junto con datos no protegidos, pero los datos protegidos:

- Sigue el tiempo de retención configurado para el bloqueo de evidencias. Potencialmente infinitamente
- Conserva la calidad original de las grabaciones, incluso si se ha configurado el arreglo para datos no protegidos

Cuando un operador crea bloqueos, el tamaño mínimo de una secuencia es el periodo en el que la base de datos divide archivos grabados, que, de forma predeterminada, son secuencias de una hora. Puede cambiar esto, pero requiere que personalice el archivo RecorderConfig.xml en el servidor de grabaciones. Si una secuencia pequeña abarca dos periodos de una hora, el sistema bloquea la grabación en ambos periodos.

En el registro de auditoría de Management Client, puede ver cuándo un usuario crea, edita o elimina bloqueos de evidencias.

Cuando un disco se queda sin espacio, no afecta a 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 desencadenadas por eventos de disco lleno, para que se le notifique de manera automática.

Salvo si se están almacenando más datos durante un periodo de tiempo más prolongado y que potencialmente afecte al almacenamiento del disco, la característica de bloqueo de evidencias como tal no afecta al rendimiento del sistema.

Si mueve hardware (consulte Mover el hardware en la página 352) a otro servidor de grabaciones:

- Las grabaciones protegidas por bloqueos de evidencias permanecen en el servidor de grabaciones antiguo con el tiempo de retención que se definió cuando se creó el bloqueo de evidencias
- El usuario de XProtect Smart Client aún puede proteger datos con bloqueos de evidencias en las grabaciones que se realizaron en una cámara antes de que se moviera a otro servidor de grabación. Aunque mueva la cámara varias veces y las grabaciones se almacenen en múltiples servidores de grabación

Por defecto, todos los operadores tienen asignado el perfil de bloqueo de evidencia por defecto, pero no tienen permisos de acceso a la función. Para especificar los permisos de acceso al bloqueo de evidencias de un cometido, consulte Pestaña dispositivo (cometidos) para los ajustes de los cometidos. Para especificar el perfil del bloqueo de evidencias, consulte pestaña Información (roles) para los ajustes del rol.

En su lugar, en Management Client puede editar las propiedades del perfil del bloqueo de evidencias predeterminado y crear perfiles de bloqueo de evidencias adicionales y asignarlos a los roles.

Reglas y eventos

Reglas (explicación)

Las reglas especifican acciones que realizar con unas condiciones particulares. Ejemplo: Cuando se detecta movimiento (condición), una cámara debe empezar a grabar (acción).

Lo siguiente son **ejemplos** de lo que puede hacer con reglas:

- Iniciar y parar grabación
- Establecer velocidad de fotogramas en directo no predeterminada
- Establecer velocidad de grabación de fotogramas no predeterminada
- Iniciar y parar vigilancia de PTZ
- Poner en pausa y reanudar la vigilancia de PTZ
- Mover cámaras PTZ a posiciones específicas
- Establecer salida en estado activado/desactivado
- Enviar notificaciones por correo electrónico
- Generar entradas de registro
- Generar eventos
- Aplicar los ajustes nuevos del dispositivo, por ejemplo una resolución distinta en una cámara

- Hacer que el vídeo aparezca en los destinatarios de Matrix
- Iniciar y parar plug-ins
- Iniciar y parar la alimentación de contenido de dispositivos

Para un dispositivo significa que ese vídeo ya no se transferirá desde el dispositivo al sistema, en cuyo caso no puede ver el vídeo endirecto ni grabar vídeo. En contraste, un dispositivo en el que ha detenido la fuente de información aún puede comunicarse con el servidor de grabaciones, y puede iniciar la alimentación de contenido desde el dispositivo automáticamente por medio de una regla, en oposición a cuando el dispositivo se deshabilita manualmente en Management Client.

> Algún contenido de la regla puede requerir que ciertas características estén habilitadas para los dispositivos relevantes. Por ejemplo, una regla que especifica que una cámara no debe grabar no funciona como está previsto si la grabación no se habilita para la cámara relevante. Antes de crear una regla, Milestone le recomienda verificar que los dispositivos implicados pueden funcionar según lo esperado.

Complejidad de las reglas

Su número exacto de opciones depende del tipo de regla que quiera crear y del número de dispositivos disponibles en su sistema. Las reglas proporcionan un alto grado de flexibilidad: puede combinar condiciones de evento y de tiempo, especificar varias acciones en una sola regla y, muy a menudo, crear reglas que cubran varios o todos los dispositivos de su sistema.

Puede hacer sus reglas tan sencillas o complejas como sea necesario. Por ejemplo, puede crear reglas basadas en tiempo muy sencillas:

Ejemplo	Explicación
Regla muy simple basada en tiempo	Los lunes, entre las 08:30 y las 11:30 (condición de tiempo), la Cámara 1 y la Cámara 2 deben empezar a grabar (acción) cuando el periodo de tiempo comience, y dejar de grabar (acción de parada) cuando termine el periodo de tiempo.
Regla muy simple basada en eventos	Cuando se detecta movimiento (condición de evento) en la Cámara 1, la Cámara 1 debe empezar a grabar (acción) inmediatamente, luego deja de grabar (acción de parada) después de 10 segundos. Aunque se active una regla basada en eventos mediante un evento en un dispositivo, puede especificar qué acciones deben tener lugar en uno o más de

Ejemplo	Explicación
	otros dispositivos.
Regla que implica varios dispositivos	Cuando se detecta movimiento (condición de evento) en la Cámara 1, la Cámara 2 debe empezar a grabar (acción) inmediatamente, y la sirena conectada con Salida 3 debe sonar (acción) de inmediato. A continuación, tras 60 segundos, la Cámara 2 debe dejar de grabar (acción de parada) y la sirena conectada a la Salida 3 debe dejar de mitir sonido (acción de parada).
Regla que combina tiempo, eventos y dispositivos	Cuando se detecta movimiento (condición de evento) en la Cámara 1 y el día de la semana es sábado o domingo (condición de tiempo), la Cámara 1 y la Cámara 2 deben empezar a grabar (acción) inmediatamente, y se debe enviar una notificación al gestor de seguridad (acción). A continuación, 5 segundos después de que ya no se detecte movimiento en la Cámara 1 o la Cämara 2, las 2 cámaras deben dejar de grabar (accion de parada).

Dependiendo de las necesidades de su organización, a menudo es buena idea crear muchas reglas sencillas en lugar de unas pocas reglas complejas. Aunque signifique tener más reglas en su sistema, proporciona una forma sencilla de mantener una descripción general de lo que hacen sus reglas. Mantener las reglas sencillas ambién significa que tiene mucha más flexibilidad cuando se trata de desactivar/activar elementos individuales de las reglas. Con reglas simples, puede desactivar/activar reglas enteras cuando sea necesario.

Reglas y eventos (explicación)

Las **Reglas** son un elemento central en su sistema. Las reglas determinan ajustes muy importantes, como cuándo las cámaras deben grabar, cuándo deben vigilar las cámaras PTZ, cuándo se deben enviar notificaciones, etc.

Ejemplo: una regla que especifica que una cámara en concreto debe empezar a grabar al detectar movimiento:

Los **eventos** son elementos centrales a la hora de usar el asistente **Gestionar reglas**. En el asistente, los eventos se utilizan principalmente para desencadenar acciones. Por ejemplo, puade crear una regla que especifica que, en el caso de que se produzca un **evento** de movimiento detectado, el sistema de vigilancia debe realizar la **acción** de iniciar la grabación de vídeo desde una cámara en concreto.

Los siguientes tipos de condiciones pueden desencadenar reglas:

Nombre	Descripción
Eventos	Cuando se producen eventos en el sistema de vigilancia, por ejemplo cuando se detecta movimiento o cuando el sistema recibe información de sensores externos.
Intervalo de tiempo	Al introducir periodos de tiempo específicos, por ejemplo: `Jueves, 16 de agosto de 2007, de 07:00 a 07:59` o `cada sábado y domingo`
Intervalo de tiempo de failover	Periodos de tiempo en los que el failover está activo o inactivo.
Tiempo recurrente	Cuando establezca que una acción se ejecute en una programación detallada y recurrente. Por ejemplo: • Cada semana, el martes, cada 1 hora(s) entre 15:00 y 15:30 • El día 15 cada 3 mes(es) a las 11:45 • Todos los días cada 1 hora(s) entre 15:00 y 19:00 La hora se basa en la configuración de la hora local del servidor en el que está instalado Management Client.

Puede trabajar con lo siguiente en **Reglas y Eventos**:

- **Reglas**: Las reglas son un elemento central del sistema. El comportamiento de su sistema de vigilancia viene determinado en gran medida por reglas. Al crear una regla, puede trabajar con todos los tipos de eventos
- **Perfiles temporales**: Los perfiles temporales son periodos de tiempo definidos en Management Client. Utilícelos cuando cree reglas en Management Client, por ejemplo para crear una regla que especifica que una determinada acción debe tener lugar en un perfil temporal determinado
- **Perfiles de notificación**: Puede utilizar perfiles de notificación para configurar notificaciones de correo preparadas para usar, que se pueden desencadenar automáticamente con una regla, por ejemplo, cuando se produce un evento concreto

- **Eventos definidos por el usuario**: Los eventos definidos por el usuario son eventos personalizados que permiten a los usuarios desencadenar manualmente eventos en el sistema o reaccionar a entradas desde el sistema
- **Eventos de análisis**: Los eventos de análisis son datos recibidos de un proveedor externo de análisis de contenido de vídeo (VCA) de terceros. Puede utilizar eventos de análisis como base para alarmas
- **Eventos genéricos**: Los eventos genéricos le permiten desencadenar acciones en el servidor de eventos XProtect enviando cadenas sencillas por medio de la red IP a su sistema

Perfiles temporales (explicación)

> La funcionalidad disponible depende del sistema que esté utilizando. Vea la lista completa de características, que está disponible en la página de descripción del producto en el sitio web Milestone (https://www.milestonesys.com/solutions/platform/product-index/).

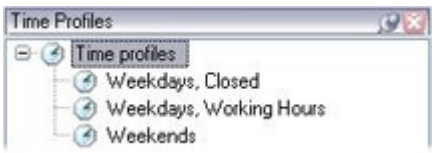
Los perfiles temporales son periodos de tiempo definidos por el administrador. Puede utilizar perfiles temporales al crear reglas, por ejemplo, una regla que especifique que una determinada acción debe tener lugar en un periodo de tiempo concreto.

Los perfiles temporales también se asignan a roles, junto con perfiles de Smart Client. De forma predeterminada, a todos los roles se les asigna el perfil temporal predeterminado **Siempre**. Esto significa que los miembros de los cometidos con este perfil temporal predeterminado no tienen límites de tiempo para sus permisos de usuario en el sistema. También puede asignar un perfil temporal alternativo a un rol.

Los perfiles temporales son muy flexibles: puede basarlos en uno o más periodos de tiempo únicos, uno o más periodos de tiempo recurrentes o una combinación de tiempos úncos y recurrentes. Muchos usuarios pueden estar familiarizados con los conceptos de periodos de tiempo únicos y recurrentes de aplicaciones de calendario, como el de Microsoft® Outlook.

Los perfiles temporal siempre se aplican en la hora local. Esto significa que, si su sistema tiene servidores de grabación ubicados en distintas zonas horarias, cualquier acción, por ejemplo, grabar en cámaras asociadas a los perfiles temporales, se llevan a cabo en cada hora local del servidor de grabación. Ejemplo: Si tiene un perfil temporal que cubre el periodo de 08:30 a 09:30, cualquier acción asociada en un servidor de grabaciones ubicado en Nueva York se lleva a cabo cuando la hora local sea de 08:30 a 09:30 en Nueva York, mientras que las mismas acciones en un servidor de grabaciones ubicado en Los Angeles se llevan a cabo algunas horas más tarde, cuando la hora local sea de 08:30 a 09:30 en Los Angeles.

Cree y gestione perfiles temporales expandiendo **Reglas y Eventos** > **Perfiles de tiempo**. Se abre una lista de **Perfiles temporales**. Ejemplo solo:



Para una alternativa a los perfiles temporales, consulte Perfiles temporales de duración de día (explicación).

Perfiles temporales de duración de día (explicación)

Cuando coloca cámaras en el exterior, a menudo debe bajar la resolución de las cámaras, habilitar el ajuste blanco/negro o cambiar otros ajustes cuando oscurece o cuando hay luz. Cuanto más lejos del norte o el sur del ecuador se coloquen las cámaras, más varía la hora del amanecer y el ocaso durante el año. Esto hace que no sea posible utilizar perfiles temporales fijos normales para ajustar los ajustes de la cámara acorde a las condiciones lumínicas.

En tales situaciones, puede crear perfiles temporales de duración de día en lugar de definir el amanecer y el ocaso en un área geográfica especificada. Por medio de coordenadas geográficas, el sistema calcula la hora del amanecer y del ocaso, incluso incorporando el horario de verano a diario. Como resultado, el perfil temporal automáticamente sigue los cambios anuales de la salida y la puesta de sol en el área seleccionada, lo que garantiza que el perfil solo esté activo cuando es necesario. Todas las horas y fechas se basan en los ajustes de hora y fecha del servidor de gestión. También puede establecer una compensación positiva o negativa (en minutos) para el momento de inicio (amanecer) y de finalización (ocaso). La compensación para la hora de inicio y final puede ser idéntica o diferente.

Puede utilizar perfiles de todo el día tanto cuando crea reglas como cuando crea roles.

Perfiles de notificación (explicación)

Los perfiles de notificación le permiten configurar notificaciones de correo electrónico ya preparadas. Las notificaciones pueden desencadenarse automáticamente mediante una regla, por ejemplo cuando se produce un evento concreto.

Al crear el perfil de notificación, especifica el texto del mensaje y decide si quiere incluir imágenes fijas y videoclips AVI en las notificaciones de correo electrónico.

> ⚠ Puede tener que deshabilitar cualquier escáner de correo electrónico que pudiera impedir que la aplicación envíe notificaciones de correo electrónico.

Requisitos para crear perfiles de notificación

Antes de poder crear perfiles de notificación, debe especificar ajustes del servidor de correo para las notificaciones de correo electrónico.

Puede proteger la comunicación con el servidor de correo si instala los certificados de seguridad necesarios en el servidor de correo.

Si quiere que las notificaciones de correo electrónico sean capaces de incluir clips de películas AVI, primero debe especificar los ajustes de compresión:

1. Vaya a **Herramientas** > **Opciones**. Esto abre la ventana **Opciones**.
2. Configure el servidor de correo en la pestaña **Servidor de correo** (Pestaña Servidor de correo (opciones) en la página 401) y los ajustes de compresión en la pestaña **Generación de AVI** Pestaña Generación de AVI (opciones) en la página 402.

Eventos definidos por el usuario (explicación)

Si el evento que requiere no está en la lista **Descripción general de eventos**, puede crear sus propios eventos definidos por el usuario. Utilice esos eventos definidos por el usuario para integrar otros sistemas con el sistema de vigilancia.

Con eventos definidos por el usuario, puede usar datos recibidos de un sistema de control de acceso de terceros como eventos en el sistema. Más tarde los eventos pueden desencadenar acciones. De este modo, puede, por ejemplo, empezar a grabar vídeo desde cámaras relevantes cuando alguien entra en un edificio.

También puede usar eventos definidos por el usuario para desencadenar manualmente eventos mientras visualiza vídeo en directo en XProtect Smart Client o automáticamente si los utiliza en reglas. Por ejemplo, cuando un se produce un evento 37 definido por el usuario, la cámara PTZ 224 debe detener dejar de vigilar e ir a la posición predefinida 18.

Por medio de los roles, define cuáles de sus usuarios son capaces de desencadenar los eventos definidos por el usuario. Puede utilizar eventos definidos por el usuario de dos formas y al mismo tiempo si fuera necesario:

Eventos	Descripción
Para proporcionar la capacidad de desencadenar eventos manualmente en XProtect Smart Client	En este caso, los eventos definidos por el usuario permiten a los usuarios finales desencadenar manualmente eventos mientras visualizan vídeo en directo en XProtect Smart Client. Cuando un evento definido por el usuario se produce debido a que un usuario de XProtect Smart Client lo desencadena manualmente, una regla puede desencadenar que una o más acciones tengan lugar en el sistema.
Para proporcionar la capacidad de desencadenar eventos mediante la API	En este caso, puede desencadenar eventos definidos por el usuario fuera del sistema de vigilancia. Utilizar eventos definidos por el usuario de este modo requiere una API (Interfaz del programa de la aplicación) separada. Se utiliza un conjunto de componentes para crear o personalizar aplicaciones de software al desencadenar el evento definido por el usuario. Se requiere la autenticación mediante Active Directory para usar eventos definidos por el usuario de esta manera. Esto garantiza que incluso si los eventos definidos por el usuario pueden desencadenarse desde fuera del sistema de vigilancia, solo los usuarios autorizados deben hacerlo.

Eventos	Descripción
	Asimismo, los eventos definidos por el usuario pueden, mediante API, asociarse a metadatos, definiendo ciertos dispositivos o grupos de dispositivos. Esto es muy útil cuando se usan eventos definidos por el usuario para desencadenar reglas: evita tener una regla para cada dispositivo, básicamente haciendo lo mismo. Ejemplo: Una empresa utiliza control de acceso, con 35 entradas, cada una de ellas con un dispositivo de control de acceso device. Cuando un dispositivo de control de acceso se activa, se desencadena un evento definido por el usuario en el sistema. Este evento definido por el usuario se utiliza en una regla para iniciar la grabación en una cámara asociada al dispositivo de control de acceso activado. En los metadatos se define qué cámara está asociada con qué regla. De este modo, la empresa no necesita tener 35 eventos definidos por el usuario y 35 reglas desencadenadas por los eventos definidos por el usuario. Un único evento definido por el usuario y una única regla son suficiente. Al utilizar eventos definidos por el usuario de este modo, puede que no siempre quiera que estén disponibles para su desencadenamiento manual en XProtect Smart Client. Puede utilizar roles para definir qué eventos definidos por el usuario deben ser visibles en XProtect Smart Client.

Eventos de análisis (explicación)

Los eventos de análisis son normalmente datos recibidos de un proveedor externo de análisis de contenido de vídeo (VCA) de terceros.

Utilizar eventos de análisis como para para alarmas es básicamente un proceso de tres pasos:

- Parte uno, habilitar la característica de los eventos de análisis y configurar su seguridad. Utilice una lista de direcciones permitidas para controlar quién puede enviar datos de eventos al sistema y en qué puerto escucha el servidor
- Parte dos, crear el evento de análisis, posiblemente con una descripción del evento, y probarlo
- Parte tres, utilizar el evento de análisis como la fuente de una definición de alarmas

Configure eventos de análisis en la lista **Reglas y Eventos** en el panel **Navegación por el centro**.

Para utilizar eventos basados en VCA, se requiere una herramienta VCA de terceros para proporcionar datos al sistema. La herramienta de VCA que utilice depende totalmente de usted, siempre que los datos suministrados por la herramienta se ajusten al formato. Este formato se explica en la Documentación de MIP SDK en eventos de análisis.

Contacto con el proveedor de su sistema para tener más detalles. Las herramientas de VCA de terceros las desarrollan socios independientes que proporcionan soluciones basadas en una plataforma Milestone abierta. Estas soluciones pueden afectar al rendimiento en el sistema.

Eventos genéricos (explicación)

Los eventos genéricos le permiten desencadenar acciones en el servidor de eventos XProtect enviando cadenas sencillas por medio de la red IP a su sistema.

Puede utilizar cualquier hardware o software que pueda enviar cadenas mediante TCP o UDP para desencadenar eventos genéricos. El sistema puede analizar los paquetes de datos de TCP o UDP recibidos, y automáticamente desencadena eventos genéricos cuando se cumplen los criterios específicos. De este modo, puede integrar su sistema con fuentes externas, por ejemplo, sistemas de control de acceso y sistemas de alarma. El objetivo es permitir que tantas fuentes externas como sea posible interactúen con el sistema.

Con el concepto de fuentes de datos, evita tener que adaptar herramientas de terceros para cumplir los estándares de su sistema. Con fuentes de datos, puede comunicarse con un elemento concreto de hardware o software en un puerto IP específico y ajustar cuántos bytes de los que llegan a ese puerto se interpretan. Cada tipo de evento genérico se empareja con una fuente de datos y crea un lenguaje que se utiliza para comunicarse con un elemento concreto de hardware o software.

Trabajar con fuentes de datos requiere conocimiento general de redes IP y conocimiento específico del hardware o el software individual desde el que quiere interactuar. Hay muchos parámetros que puede usar y no hay soluciones comerciales listas para hacerlo. Básicamente, el sistema proporciona las herramientas, pero no la solución. A diferencia de los eventos definidos por el usuario, los eventos genéricos no tienen autenticación. Esto hace que sea más fácil desencadenarlos, pero, para evitar poner en peligro la seguridad, solo se aceptan eventos del host local. Puede permitir otras direcciones IP de clientes desde la pestaña **Eventos genéricos** del menú **Opciones**.

Webhooks (explicado)

Los webhooks son solicitudes HTTP que permiten a las aplicaciones web comunicarse entre sí y facilitan el envío de datos en tiempo real de una aplicación a otra al producirse un evento predefinido; por ejemplo, enviar datos de eventos a un punto final de webhook predefinido cuando un usuario inicia sesión en el sistema o cuando una cámara informa de un error.

Un punto final de webhook (webhook URL) es la dirección predefinida a la que se enviarán los datos del evento, de forma similar a un número de teléfono unidireccional.

Se pueden utilizar webhooks para crear integraciones que se suscriban a eventos seleccionados en XProtect. Al activarse un evento, se envía un POST HTTP al punto final del webhook que se haya definido para ese evento. El cuerpo del POST HTTP contiene los datos del evento en JSON.

Los webhooks no sondean el sistema en busca de datos o eventos activados, sino que el sistema envía los datos del evento al punto final del webhook al producirse un evento, lo que hace que los webhooks requieran menos recursos y sean más rápidos de configurar en comparación con las soluciones de polling.

Los webhooks pueden ajustarse para integrarse con o sin el uso de secuencias de comandos de código.

> ⚠ Debe verificar que los datos de eventos enviados desde XProtect cumplen con la legislación vigente sobre protección de datos y privacidad de su país.

La funcionalidad Webhooks está instalada por defecto y lista para su uso en XProtect 2023R1 o posteriormente y muestra la acción **Webhooks** en la pestaña **Reglas** en el Management Client. con su propio contenido.

Si desea más información, consulte Webhooks en XProtect

Alarmas

Alarmas (explicación)

Esta característica solo funciona si tiene XProtect Event Server instalado.

Este artículo describe cómo configurar las alarmas para que aparezcan en el sistema, activadas por eventos.

Basándose en la funcionalidad que se maneja en el servidor de eventos, la función de alarmas proporciona una visión general centralizada, control y escalabilidad de las alarmas en cualquier número de instalaciones (incluyendo cualquier otro sistema XProtect) en toda su organización. Puede configurarlo para generar alarmas basadas en cualquiera de los dos elementos:

- **Eventos relacionados con el sistema interno**

  Por ejemplo, el movimiento, el servidor que responde/no responde, los problemas de archivo, la falta de espacio en el disco y más.

- **Eventos externos integrados**

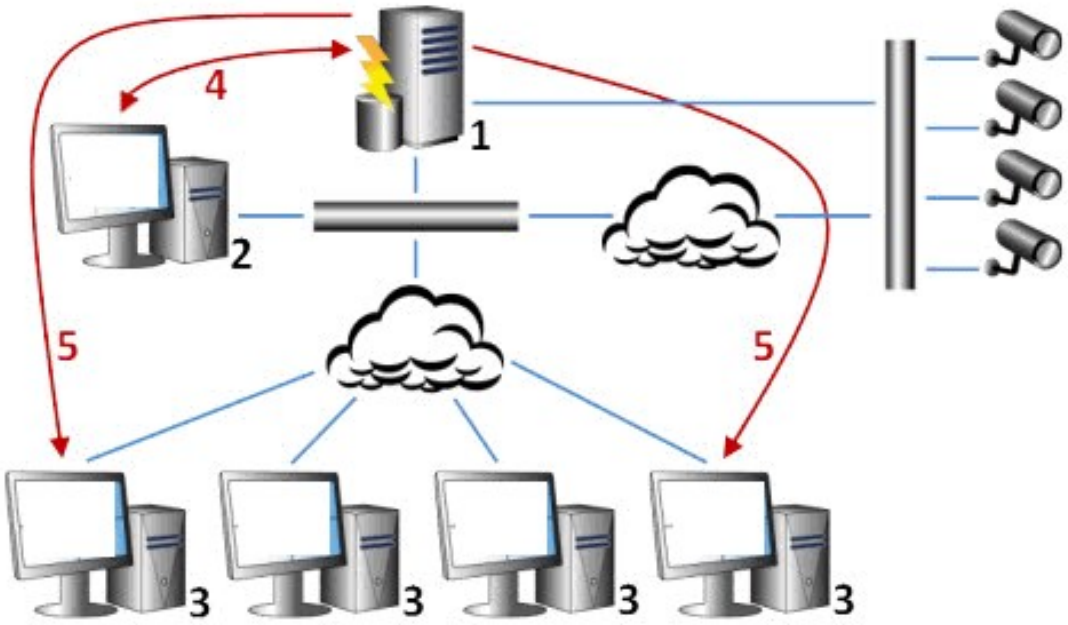
  Este grupo está formado por varios tipos de eventos externos:

  - **Eventos analíticos**

    Normalmente, los datos se reciben de un proveedor externo de análisis de contenido de vídeo (ACV).

  - **MIP eventos de plug-in**

    A través del MIP SDK un proveedor externo puede desarrollar plug-ins personalizados (por ejemplo, la integración a sistemas de control de acceso externos o similares) para su sistema.



Leyenda:

1. Sistema de vigilancia
2. Management Client
3. XProtect Smart Client
4. Configuración de alarma
5. Flujo de datos de alarma

Gestiona y delega las alarmas en la lista de alarmas en XProtect Smart Client. También puede integrar las alarmas con el plano inteligente de XProtect Smart Client y la funcionalidad del plano.

Configuración de alarma

La configuración de la alarma incluye:

- Configuración dinámica de gestión de alarmas basada en cometidos
- Resumen técnico central de todos los componentes: servidores, cámaras y unidades externas
- Configuración del registro central de todas las alarmas entrantes y de la información del sistema
- Manejo de plug-ins, lo que permite la integración personalizada de otros sistemas, por ejemplo, control de acceso externo o sistemas basados en VCA

En general, las alarmas se controlan en función de la visibilidad del objeto que las provoca. Esto significa que hay cuatro aspectos posibles que pueden desempeñar un cometido con respecto a las alarmas y a quién puede controlarlas/gestionarlas y en qué grado:

Nombre	Descripción
Visibilidad de la fuente/dispositivo	Si el dispositivo que causa la alarma no está configurado para ser visible para el cometido del usuario, éste no podrá ver la alarma en la lista de alarmas en XProtect Smart Client.
El derecho a activar eventos definidos por el usuario	Este permiso determina si el cometido del usuario puede activar eventos seleccionados definidos por el usuario en XProtect Smart Client.
Plug-ins externos	Si hay algún plug-in externo configurado en su sistema, éste podría controlar los permisos de los usuarios para manejar las alarmas.
Derechos generales de cometido	Determinar si el usuario está autorizado a ver solo las alarmas o también a gestionarlas. Lo que un usuario de **Alarmas** puede hacer con las alarmas depende del cometido del usuario y de los ajustes configurados para ese cometido en particular.

En la pestaña **Alarmas y Eventos** en **Opciones**, puede especificar la configuración de alarmas, eventos y registros.

Plano inteligente

Plano inteligente (explicación)

En XProtect® Smart Client, la función de plano inteligente le permite ver y acceder a los dispositivos en varios lugares del mundo de forma geográficamente correcta. A diferencia de los planos, en los que tenía un plano diferente para cada lugar, el plano inteligente le ofrece la visión general en una sola vista.

La siguiente configuración de la función de plano inteligente se realiza en Management Client:

- Configurar los fondos geográficos que puede elegir para su plano inteligente. Esto incluye la integración de su plano inteligente con uno de los siguientes servicios:
  - Bing Maps
  - Google Maps
  - Milestone Map Service
  - OpenStreetMap
- Habilitar Bing Maps o Google Maps en XProtect Management Client o en XProtect Smart Client
- Habilitar la edición de planos inteligentes, incluidos los dispositivos, en XProtect Smart Client
- Posicionar sus dispositivos geográficamente en XProtect Management Client
- Configurar su plano inteligente con Milestone Federated Architecture

Integración de planos inteligentes con Google Maps (explicación)

Para integrar Google Maps en su plano inteligente, necesita una clave de Maps Static API de Google. Para obtener la clave API, primero debe crear una cuenta de facturación de Google Cloud. Se le factura en función del volumen de cargas de planos por mes.

Una vez que tenga la clave API, debe introducirla en XProtect Management Client. Consulte también Habilitar Bing Maps o Google Maps en Management Client en la página 331.

Si está detrás de un cortafuegos restrictivo, es importante permitir el acceso a los dominios utilizados. Es posible que tenga que permitir el tráfico de salida para el Google Maps utilizando maps.googleapis.com en cada máquina en la que se ejecute el Smart Client.

Si desea más información, consulte:

- Google Maps Platform - primeros pasos: https://cloud.google.com/maps-platform/
- Guía a facturación de Google Maps Platform: https://developers.google.com/maps/billing/gmp-billing
- Guía para desarrolladores de la Maps Static API: https://developers.google.com/maps/documentation/maps-static/dev-guide

Añadir firma digital a la clave Maps Static API

Si espera que los operadores XProtect Smart Client realicen más de 25 000 solicitudes de planos al día, necesita una firma digital para su clave de Maps Static API. La firma digital permite a los servidores de Google verificar que cualquier sitio que genere solicitudes utilizando su clave API está autorizado a hacerlo. Sin embargo, independientemente de los requisitos de uso, Google recomienda utilizar una firma digital como capa de seguridad adicional. Para obtener la firma digital, debe recuperar un secreto de firma URL. Si desea más información, consulte https://developers.google.com/maps/documentation/maps-static/get-api-key#dig-sig-manual.

Integración de planos inteligentes con Bing Maps (explicación)

Para integrar Bing Maps en su plano inteligente, necesita una Clave Básica o una Clave Empresarial. La diferencia es que las claves básicas son gratuitas, pero permiten un número limitado de transacciones antes de que éstas sean facturables o se deniegue el acceso al servicio de planos. La clave empresarial no es gratuita, pero permite un número ilimitado de transacciones.

Si desea más información acerca de Bing Maps, consulte https://www.microsoft.com/en-us/maps/licensing/.

Una vez que tenga la clave API, debe introducirla en XProtect Management Client. Consulte Habilitar Bing Maps o Google Maps en Management Client en la página 331.

Si está detrás de un cortafuegos restrictivo, es importante permitir el acceso a los dominios utilizados. Es posible que tenga que permitir el tráfico de salida para los planos de Bing utilizando *.virtualearth.net en cada máquina en la que se ejecute el Smart Client.

Archivos de planos inteligentes en caché (explicación)

Si está utilizando Google Maps como su entorno geográfico, los archivos no están en el caché.

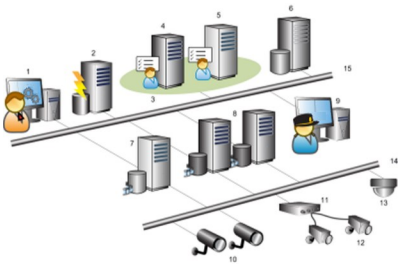
Los archivos que se utilizan para el fondo geográfico se obtienen de un servidor de fichas. El tiempo que los archivos se almacenan en la carpeta de caché depende del valor seleccionado en la lista **Archivos de planos inteligentes eliminados en caché** del cuadro de diálogo **Ajustes** en XProtect Smart Client. Los archivos se almacenan:

- Indefinidamente (**Nunca**)
- Durante 30 días si no se utiliza el archivo (**Cuando no se utiliza durante 30 días**)
- Cuando el operador sale XProtect Smart Client (**Al salir**)

Cuando cambie la dirección del servidor de fichas, se creará automáticamente una nueva carpeta de caché. Los archivos de planos anteriores se conservan en la carpeta de caché asociada en su ordenador local.

Arquitectura

Una configuración de sistema distribuida



Ejemplo de una configuración de sistema distribuido. El número de cámaras, servidores de grabación y clientes conectados puede ser tan alto como necesite.

> Todos los ordenadores de una configuración distribuida deben estar en un dominio o en un grupo de trabajo.

Leyenda:

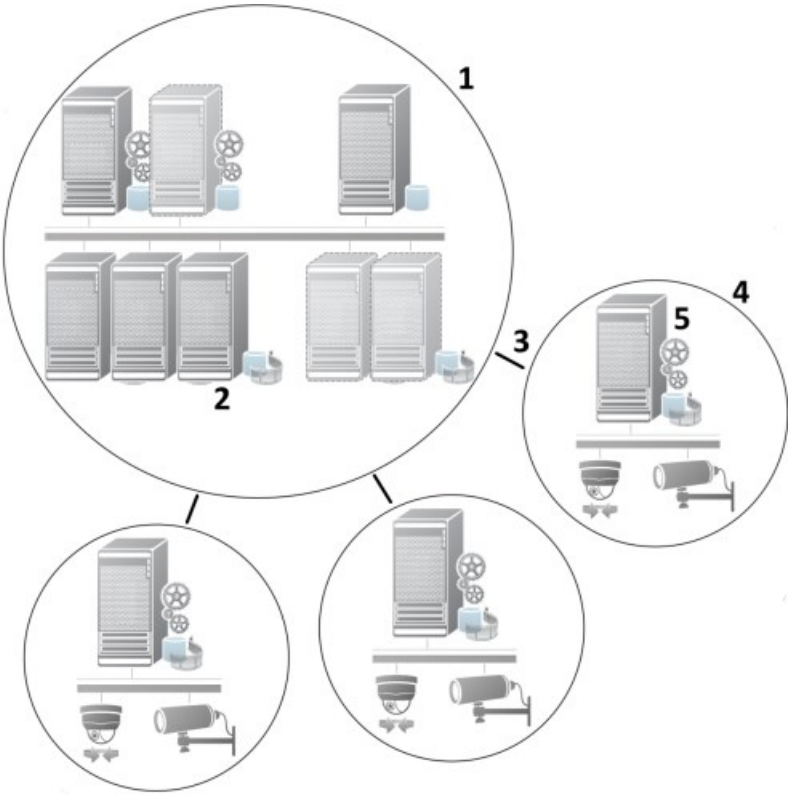
1. Management Client(s)
2. Servidor de evento
3. Clúster de Microsoft
4. Servidor de gestión
5. Servidor de gestión de failover
6. Servidor con SQL Server
7. Servidor de grabación failover
8. Servidor(es) de grabación
9. XProtect Smart Client(s)
10. Cámaras de vídeo IP
11. Codificador de vídeo
12. Cámaras analógicas
13. Cámara IP PTZ
14. Red de la cámara
15. Red de servidores

Milestone Interconnect (explicación)

La funcionalidad disponible depende del sistema que esté utilizando. Vea la lista completa de características, que está disponible en la página de descripción del producto en el sitio web Milestone (https://www.milestonesys.com/solutions/platform/product-index/).

Milestone Interconnect™ le permite integrar una serie de instalaciones más pequeñas, físicamente fragmentadas e instalaciones remotas XProtect con un sitio central XProtect Corporate. Puede instalar estos sitios más pequeños, llamados sitios remotos, en unidades móviles, por ejemplo, barcos, autobuses o trenes. Esto significa que estos sitios no necesitan estar permanentemente conectados a una red.

La siguiente ilustración muestra cómo podría configurar Milestone Interconnect en su sistema:



1. Milestone Interconnect sitio central XProtect Corporate
2. Milestone Interconnect drivers (maneja la conexión entre los servidores de grabación de los sitios centrales y el sitio remoto, debe ser seleccionado en la lista de drivers cuando se agregan los sistemas remotos a través del asistente **Añadir Hardware**)
3. Milestone Interconnect conexión

4. Milestone Interconnect sitio remoto (el sitio remoto completo con la instalación del sistema, los usuarios, las cámaras, etc.)
5. Milestone Interconnect sistema remoto (la instalación técnica real en el sitio remoto)

Los sitios remotos se añaden al sitio central con el asistente para **Añadir hardware** desde el sitio central (consulte Añadir un sitio remoto a su sitio central Milestone Interconnect en la página 324).

Cada sitio remoto funciona de forma independiente y puede realizar cualquier tarea de vigilancia normal. Dependiendo de las conexiones de red y de los permisos de usuario adecuados (consulte Asignar permisos de usuario en la página 325), Milestone Interconnect le ofrece la visualización directa en directo de las cámaras del sitio remoto y la reproducción de las grabaciones del sitio remoto en el sitio central.

El sitio central solo puede ver y acceder a los dispositivos a los que la cuenta de usuario especificada (al añadir el sitio remoto) tiene acceso. Esto permite a los administradores del sistema local controlar qué dispositivos deben estar disponibles para el sitio central y sus usuarios.

En el sitio central, puede ver el estado propio del sistema para las cámaras interconectadas, pero no directamente el estado del sitio remoto. En cambio, para supervisar el sitio remoto, puede utilizar los eventos del sitio remoto para activar alarmas u otras notificaciones en el sitio central (consulte Configurar el sitio central para que responda a los eventos de los sitios remotos en la página 327).

También le ofrece la posibilidad de transferir las grabaciones de los sitios remotos al sitio central basándose en eventos, reglas/programas o solicitudes manuales de los usuarios de XProtect Smart Client.

Solo los sistemas XProtect Corporate pueden funcionar como sitios centrales. Todos los demás productos pueden actuar como sitios remotos, incluyendo XProtect Corporate. Difiere de una configuración a otra qué versiones, cuántas cámaras y cómo se gestionan los dispositivos y los eventos que se originan en el sitio remoto, si es que lo hacen, por el sitio central. Para obtener más detalles sobre cómo interactúan los productos específicos XProtect en una configuración Milestone Interconnect, vaya al sitio web de Milestone Interconnect (https://www.milestonesys.com/solutions/hardware-and-add-ons/milestone-addons/interconnect/).

Seleccionar Milestone Interconnect o Milestone Federated Architecture (explicación)

En un sistema físicamente distribuido en el que los usuarios del sitio central necesitan acceder al vídeo 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 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 remotos es inestable
- Usted o su organización desean utilizar otro producto XProtect en los sitios remotos
- La red utiliza diferentes dominios o grupos de trabajo
- Hay muchos sitios más pequeños

Milestone Interconnect y licencia

Para ejecutar Milestone Interconnect, necesita Milestone Interconnect licencias de cámaras en su sitio central para ver vídeo de los dispositivos de hardware en sitios remotos. El número de Milestone Interconnect licencias de cámara necesarias depende del número de dispositivos de hardware en los sitios remotos de los que se desea recibir datos. Únicamente XProtect Corporate puede desempeñar la función de ubicación central.

El estado de sus licencias de cámara Milestone Interconnect se encuentra en la página de **Información de licencias** del sitio central.

Milestone Interconnect ajustes (explicación)

Hay tres formas de ejecutar Milestone Interconnect. La forma de ejecutar la configuración depende de la conexión de red, de la forma de reproducir las grabaciones y de si se recuperan las grabaciones remotas y en qué medida.

En la siguiente, se describen las tres configuraciones más probables:

Reproducción directa desde sitios remotos (buenas conexiones de red)

La configuración más sencilla. El sitio central está continuamente en línea con sus sitios remotos y los usuarios del sitio central reproducen las grabaciones remotas directamente desde los sitios remotos. Para ello es necesario utilizar la opción **Reproducir grabaciones desde el sistema remoto** (consulte Habilitar la reproducción directamente desde la cámara del sitio remoto en la página 325).

Recuperación basada en reglas o en XProtect Smart Client de secuencias de grabación remotas seleccionadas desde sitios remotos (conexiones de red limitadas periódicamente)

Se utiliza cuando las secuencias de grabación seleccionadas (procedentes de sitios remotos) deben almacenarse de forma centralizada para garantizar la independencia de los sitios remotos. La independencia es crucial en caso de fallo o restricciones de la red. Los ajustes de recuperación de grabaciones remotas se configuran en la pestaña de **Recuperación remota** (consulte Pestaña Recuperación remota en la página 448).

La recuperación de grabaciones remotas puede iniciarse desde el XProtect Smart Client cuando sea necesario o se puede establecer una regla. En algunos escenarios, los sitios remotos están en línea y en otros, fuera de línea la mayor parte del tiempo. A menudo esto es específico del sector. En algunos sectores es habitual que la sede central esté permanentemente en línea con sus sedes remotas (por ejemplo, una sede comercial (sede central) y varias tiendas (sitios remotos). En otros sectores, como el del transporte, los lugares remotos son

móviles (por ejemplo, autobuses, trenes, barcos, etc.) y solo pueden establecer una conexión de red de forma aleatoria. Si la conexión de red falla durante la recuperación de una grabación remota iniciada, el trabajo continúa en la siguiente oportunidad.

Si el sistema detecta una recuperación automática, o una solicitud de recuperación del XProtect Smart Client, fuera del intervalo de tiempo que especificó en la pestaña **Recuperación remota**, se acepta, pero no se inicia hasta que se alcance el intervalo de tiempo seleccionado. Los nuevos trabajos de recuperación de grabaciones remotas se pondrán en cola y comenzarán cuando se alcance el intervalo de tiempo permitido. Puede ver los trabajos pendientes de recuperación de grabaciones remotas desde el **Panel del sistema** -> **Tareas actuales**.

Tras un fallo de conexión, las grabaciones remotas que faltan se recuperan por defecto de los sitios remotos

Utiliza sitios remotos como un servidor de grabación utiliza el almacenamiento edge en una cámara. Por lo general, los sitios remotos están en línea con su sitio central, alimentándolo con una transmisión en directo que el sitio central graba. Si la red falla por alguna razón, el sitio central pierde las secuencias de grabación. Sin embargo, una vez restablecida la red, la sede central recupera automáticamente las grabaciones remotas que cubren el periodo de inactividad. Esto requiere el uso de la opción **Recuperar automáticamente las grabaciones remotas cuando se restablezca la conexión** (consulte Recuperar grabaciones a distancia de la cámara del sitio remoto en la página 326) en la pestaña **Grabar** de la cámara.

Puede mezclar cualquiera de las soluciones anteriores para adaptarse a las necesidades especiales de su organización.

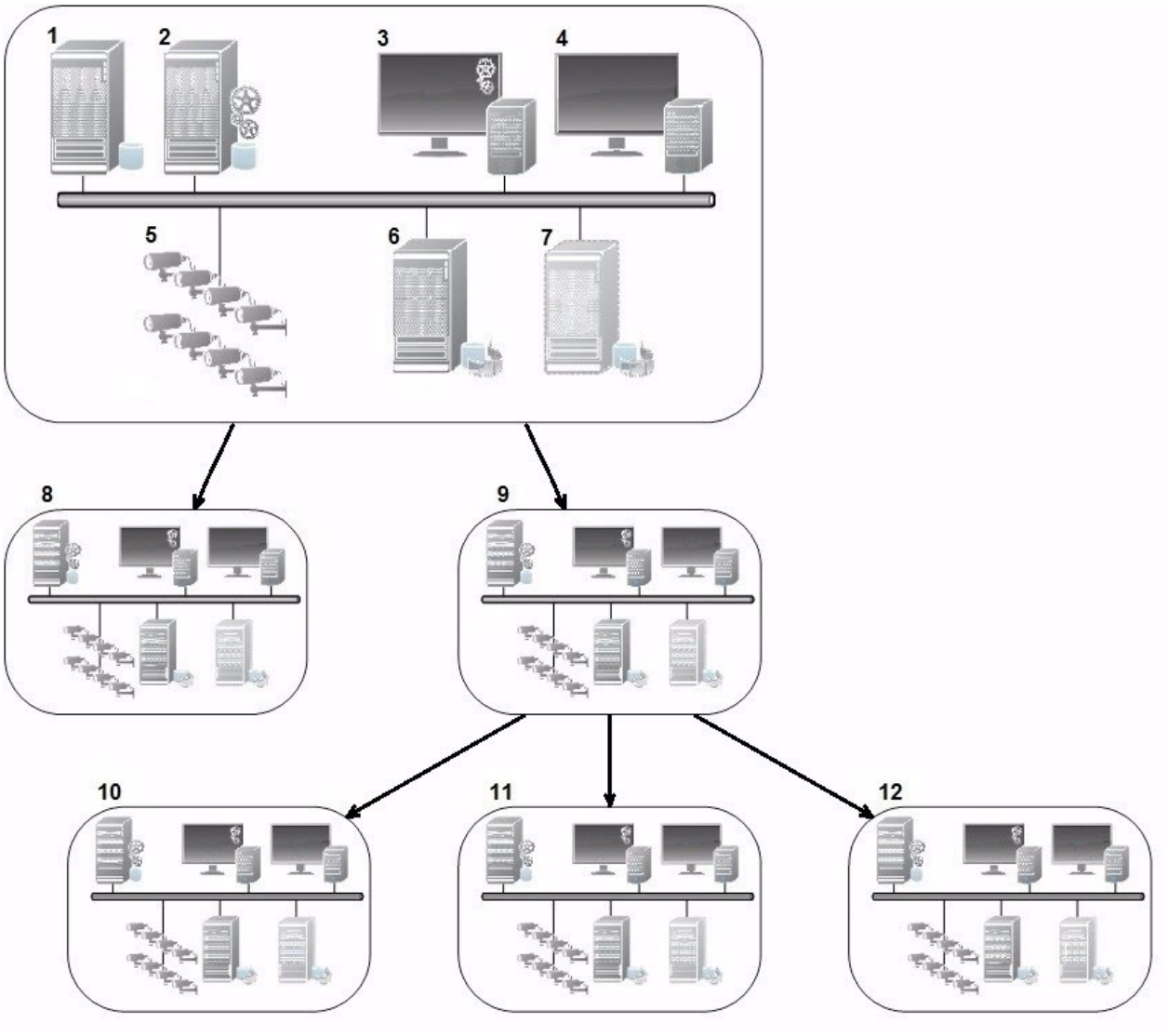
Configuración de Milestone Federated Architecture

XProtect Expert solo pueden ser federados como sitios secundarios.

Milestone Federated Architecture vincula varios sistemas estándar individuales en una jerarquía de sitios federados de sitios principales/secundarios. Los usuarios de los clientes con permisos suficientes tienen un acceso perfecto al vídeo, al audio y a otros recursos en los sitios individuales. Los administradores pueden gestionar de forma centralizada todos los sitios de la versión 2018 R1 y posteriores dentro de la jerarquía federada, basándose en los permisos de administrador para 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.

Milestone Federated Architecture se configura con un sitio central (sitio superior) y un número ilimitado de sitios federados (consulte Configurar su sistema para ejecutar sitios federados en la página 318). Cuando haya iniciado sesión en un sitio, podrá acceder a información sobre todos sus sitios secundarios y los sitios secundarios de los sitios secundarios. El enlace entre dos sitios se establece, cuando se solicita el enlace desde el sitio principal (consulte Añadir sitio a la jerarquía en la página 320). Un sitio secundario solo puede estar vinculado a un sitio principal. Si no es el administrador del sitio secundario cuando lo añade a la jerarquía de sitios federados, la solicitud debe ser aceptada por el administrador del sitio secundario.



Los componentes de una configuración Milestone Federated Architecture:

1. Servidor con 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 adjuntos, los sitios secundarios de los sitios secundarios, etc. La jerarquía de sitios federados tiene una sincronización programada entre sitios, así como una sincronización cada vez que el administrador del sistema añade o elimina un sitio. Cuando el sistema sincroniza la jerarquía, lo hace nivel a nivel, cada nivel reenvía y devuelve la comunicación, hasta llegar al servidor que solicita la información. El sistema envía menos de 1MB cada vez. Dependiendo del número de niveles, los cambios en una jerarquía pueden tardar en hacerse visibles en el Management Client. No puede programar sus propias sincronizaciones.

Tráfico de datos

El sistema envía datos de comunicación o de configuración cuando un usuario o un administrador ve un vídeo en directo o grabado o configura un sitio. La cantidad de datos depende de qué y cuánto se esté viendo o configurando.

Milestone Federated Architecture con otros productos y requisitos del sistema

- Abrir el Management Client en un Milestone Federated Architecture es compatible con tres versiones principales, incluida la actual que se está publicando. En una configuración Milestone Federated Architecture más allá de ese ámbito, necesita una Management Client separada que coincida con la versión del servidor.
- Si el sitio central utiliza XProtect Smart Wall, también puede utilizar las características de XProtect Smart Wall en la jerarquía del sitio federado.

  Consulte también el manual para XProtect Smart Wall.
- Si el sitio central utiliza XProtect Access y el usuario de XProtect Smart Client inicia sesión en un sitio en una jerarquía de sitios federados, 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 principales
- Milestone Federated Architecture no requiere licencias adicionales
- Si desea más información sobre los casos de uso y las ventajas, consulte el libro blanco sobre Milestone Federated Architecture.

Establecer una jerarquía de sitios federados

Antes de empezar a construir la jerarquía en el Management Client, Milestone recomienda que planifique cómo quiere que sus sitios se vinculen entre sí.

Instala y configura cada sitio en una jerarquía federada como un sistema independiente normal con componentes de sistema estándar, ajustes, reglas, horarios, administradores, usuarios y permisos de usuario. Si ya tiene los sitios instalados y configurados y solo necesita combinarlos en una jerarquía de sitios federados, sus sistemas están listos para ser configurados.

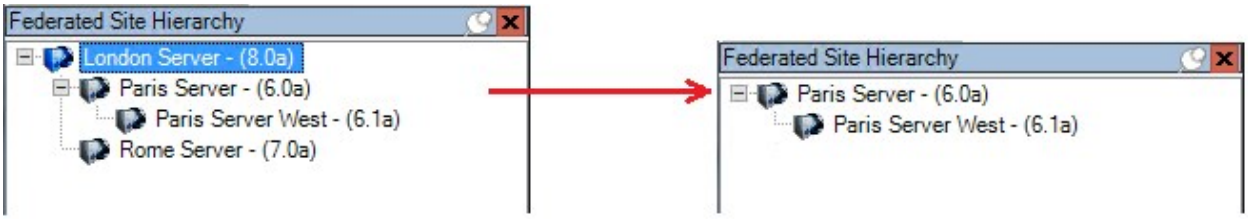
Una vez instalados los sitios individuales, debe configurarlos para que funcionen como sitios federados (consulte Configurar su sistema para ejecutar sitios federados en la página 318).

Para iniciar la jerarquía, puede iniciar sesión en el sitio que quiere que funcione como sitio central y añadir (consulte Añadir sitio a la jerarquía en la página 320) 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 a la que puede añadir más sitios para hacer crecer la jerarquía federada.

Cuando haya creado una jerarquía de sitios federados, los usuarios y administradores podrán iniciar sesión en un sitio para acceder a ese sitio y a los sitios federados que pueda tener. El acceso a los sitios federados depende de los permisos del usuario.

No hay límite en el número de sitios que puede añadir a la jerarquía federada. Además, puede tener un sitio en una versión más antigua del producto vinculado a una versión más reciente y viceversa. Los números de versión aparecen automáticamente y no se pueden borrar. El sitio en el que ha iniciado la sesión está siempre en la parte superior del panel de **Jerarquía de sitios federados** y se denomina sitio inicial.

A continuación se muestra un ejemplo de sitio federado en el Management Client. A la izquierda, el usuario ha iniciado la sesión en el sitio superior. A la derecha, el usuario se ha conectado a uno de los sitios secundarios, el Servidor París, que a su vez es el sitio principal.



Iconos de estado en Milestone Federated Architecture

Los iconos representan los posibles estados de un sitio:

Descripción	Icono
El sitio superior de toda la jerarquía es operativo.	
El sitio superior de toda la jerarquía sigue siendo operativo, pero uno o más problemas necesitan atención. Mostrado en la parte superior del icono del sitio superior.	
El sitio es operativo.	
El sitio está a la espera de ser aceptado en la jerarquía.	
El sitio se está adjuntando pero aún no está operativo.	

Puertos utilizados por el sistema

Todos los componentes de XProtect y los puertos que necesitan se enumeran a continuación. Para garantizar, por ejemplo, que el cortafuegos solo bloquea tráfico no deseado, debe especificar los puertos que usa el sistema. Solo debe habilitar estos puertos. Las listas también incluyen los puertos utilizados para los procesos locales.

Están organizados en dos grupos:

- Los **Componentes del servidor** (servicios) ofrecen su servicio en puertos concretos, que es por lo que deben escuchar solicitudes de clientes en estos puertos. Por lo tanto, estos puertos deben abrirse en el cortafuegos de Windows para conexiones entrantes y salientes
- **Componentes del cliente** (clientes) inicia conexiones con puertos concretos en los componentes del servidor. Por lo tanto, estos puertos deben abrirse para xonexiones salientes. Las conexiones salientes suelen estar abiertas de forma predeterminada en el cortafuegos de Windows

Si no se menciona nada más, los puertos para los componentes del servidor deben abrirse para conexiones entrantes, y los puertos para los componentes cliente deben abrirse para conexiones salientes.

Tenga presente que los componentes del servidor pueden actuar como clientes para otros componentes del servidor. No se enumeran explícitamente en este documento.

Los números de puerto son los números predeterminado, pero se pueden cambiar. Póngase en contacto con asistencia de Milestone, si necesita cambiar puertos que no son configurables mediante el Management Client.

Componentes del servidor (conexiones entrantes)

Cada una de las siguientes secciones enumera los puertos que deben abrirse para un servicio concreto. Para averiguar qué puertos deben estar abiertos en un ordenador concreto, debe considerar todos los servicios que se están ejecutando en el ordenador.

Management Server servicio y procesos relacionados

Número de puerto	Protocolo	Proceso	Conexiones desde...	Objetivo
80	HTTP	IIS	Todos los servidores y el XProtect Smart Client y el Management Client	La finalidad del puerto 80 y del puerto 443 es la misma. Sin embargo, qué puerto utiliza el VMS depende de si usted ha utilizado certificados para proteger la comunicación. • Cuando no se ha protegido la comunicación con certificados, el VMS utiliza el puerto 80. • Si usted ha protegido la comunicación con certificados, el VMS utiliza el puerto 443 excepto para la comunicación del servidor de eventos con el servidor de gestión. La comunicación del servidor de eventos con el servidor de gestión utiliza Windows Secured Framework (WCF) y autenticación de Windows en el puerto 80.
443	HTTPS	IIS		
6473	TCP	Management Server servicio	Management Server Manager icono de la bandeja, solo conexión local.	Mostrando estado y gestionando el servicio.
8080	TCP	Servidor de gestión	Solo conexión local.	Comunicación entre procesos internos en el servidor.
9000	HTTP	Servidor de	Recording	Servicio web para comunicación

Número de puerto	Protocolo	Proceso	Conexiones desde...	Objetivo
		gestión	Server servicios	interna entre servidores.
12345	TCP	Management Server servicio	XProtect Smart Client	Comunicación entre el sistema y los destinatarios de Matrix. Puede cargar el número de puerto en Management Client.
12974	TCP	Management Server servicio	Servicio SNMP de Windows	Comunicación con agente de extensión de SNMP. No utilice el puerto para otros fines, incluso si su sistema no aplica SNMP. En sistemas XProtect 2014 o más antiguos, el número de puerto era 6475. En sistemas XProtect 2019 R2 y más antiguos, el numero de puerto era 7475.

SQL Server servicio

Número de puerto	Protocolo	Proceso	Conexiones desde...	Objetivo
1433	TCP	SQL Server	Management Server servicio	Almacenar y recuperar configuraciones por medio de Identity Provider.
1433	TCP	SQL Server	Event Server servicio	Almacenar y recuperar eventos por medio de Identity Provider.
1433	TCP	SQL Server	Log Server servicio	Almacenar y recuperar entradas de registro por medio de Identity Provider.

Data Collector servicio

Número de puerto	Protocolo	Proceso	Conexiones desde...	Objetivo
7609	HTTP	IIS	En el ordenador del servidor de gestión: Data Collector servicios en todos los demás servidores. En otros ordenadores: Data Collector servicio en el Servidor de Gestión.	Monitor del sistema.

Event Server servicio

Número de puerto	Protocolo	Proceso	Conexiones desde...	Objetivo
1234	TCP/UDP	Event Server Servicio	Cualquier servidor que envíe eventos genéricos a su sistema XProtect.	Escuchando eventos genéricos de dispositivos o sistemas externos. Solo si la fuente de datos relevante está habilitada.
1235	TCP	Event Server servicio	Cualquier servidor que envíe eventos genéricos a su sistema XProtect.	Escuchando eventos genéricos de dispositivos o sistemas externos. Solo si la fuente de datos relevante está habilitada.
9090	TCP	Event Server servicio	Cualquier sistema o dispositivo que envía eventos de análisis a su sistema XProtect.	Escuchar eventos de análisis de dispositivos o sistemas externos.

Número de puerto	Protocolo	Proceso	Conexiones desde...	Objetivo
				Solo es relevante si la característica Eventos de análisis está habilitada.
22331	TCP	Event Server servicio	XProtect Smart Client y la Management Client	Datos de configuración, eventos, alarmas y planos.
22332	WS/WSS HTTP/HTTPS*	Event Server servicio	API Gateway y la Management Client	API de suscripción a eventos/estados y API REST de eventos
22333	TCP	Event Server servicio	MIP Plug-ins y aplicaciones.	MIP mensajería.

*Se devolverá un error 403 cuando se acceda a HTTP para acceder a un punto final solo para HTTPS.

Recording Server servicio

Número de puerto	Protocolo	Proceso	Conexiones desde...	Objetivo
25	SMTP	Recording Server Servicio	Cámaras, codificadores y dispositivos de E/S.	Escuchando mensajes de eventos de dispositivos. El puerto está deshabilitado de forma predeterminada. (Desaprobado) Habilitar esta opción abrirá un puerto para conexiones no encriptadas y no es recomendable.
5210	TCP	Recording	Servidores de	Fusión de bases de datos después

Número de puerto	Protocolo	Proceso	Conexiones desde...	Objetivo
		Server Servicio	grabación de failover.	de que se haya estado ejecutando un servidor de grabación de failover.
5432	TCP	Recording Server Servicio	Cámaras, codificadores y dispositivos de E/S.	Escuchando mensajes de eventos de dispositivos. El puerto está deshabilitado de forma predeterminada.
7563	TCP	Recording Server Servicio	XProtect Smart Client, Management Client	Recuperando flujos de vídeo y audio, comandos de PTZ.
8966	TCP	Recording Server Servicio	Recording Server Manager icono de la bandeja, solo conexión local.	Mostrando estado y gestionando el servicio.
9001	HTTP	Recording Server Servicio	Servidor de gestión	Servicio web para comunicación interna entre servidores. Si se están usando múltiples instancias del Servidor de grabaciones, cada instancia necesita su propio puerto. Los puertos adicionales serán 9002, 9003, etc.
11000	TCP	Recording Server Servicio	Servidores de grabación de failover	Agrupando el estado de los servidores de grabación.
12975	TCP	Recording Server Servicio	Servicio SNMP de Windows	Comunicación con agente de extensión de SNMP. No utilice el puerto para otros

Número de puerto	Protocolo	Proceso	Conexiones desde...	Objetivo
				fines, incluso si su sistema no aplica SNMP. En sistemas XProtect 2014 o más antiguos, el número de puerto era 6474. En sistemas XProtect 2019 R2 y más antiguos, el número de puerto era 7474.
65101	UDP	Recording Server servicio	Solo conexión local	Escuchar notificaciones de eventos de los controladores.

Además de las conexiones entrantes al servidor de Recording Server enumeradas previamente, el servicio Recording Server establece conexiones salientes a:

- Cámaras
- NVR
- Sitios remotos interconectados (ICP interconectado de Milestone)

Failover Server servicio y servicio de Failover Recording Server

Número de puerto	Protocolo	Proceso	Conexiones desde...	Objetivo
25	SMTP	Failover Recording Server Servicio	Cámaras, codificadores y dispositivos de E/S.	Escuchando mensajes de eventos de dispositivos. El puerto está deshabilitado de forma predeterminada. (Desaprobado) Habilitar esta

Número de puerto	Protocolo	Proceso	Conexiones desde...	Objetivo
				opción abrirá un puerto para conexiones no encriptadas y no es recomendable.
5210	TCP	Failover Recording Server Servicio	Servidores de grabación de failover	Fusión de bases de datos después de que se haya estado ejecutando un servidor de grabación de failover.
5432	TCP	Failover Recording Server Servicio	Cámaras, codificadores y dispositivos de E/S.	Escuchando mensajes de eventos de dispositivos. El puerto está deshabilitado de forma predeterminada.
7474	TCP	Failover Recording Server Servicio	Servicio SNMP en Windows	Comunicación con agente de extensión de SNMP. No utilice el puerto para otros fines, incluso si su sistema no aplica SNMP.
7563	TCP	Failover Recording Server Servicio	XProtect Smart Client	Recuperando flujos de vídeo y audio, comandos de PTZ.
8844	UDP	Failover Recording Server Servicio	Comunicación entre los servicios del servidor de grabación failover.	Comunicación entre los servidores.
8966	TCP	Failover Recording Server Servicio	Failover Recording Server Manager icono de la bandeja, solo conexión local.	Mostrando estado y gestionando el servicio.
8967	TCP	Failover Server	Failover Server Manager icono de la	Mostrando estado y gestionando el servicio.

Número de puerto	Protocolo	Proceso	Conexiones desde...	Objetivo
		Servicio	bandeja, solo conexión local.	
8990	TCP	Failover Server Servicio	Management Server servicio	Monitorización del estado del servicio de Failover Server.
9001	HTTP	Failover Server Servicio	Servidor de gestión	Servicio web para comunicación interna entre servidores.

Además de las conexiones entrantes al servicio del Servidor de failover/Failover Recording Server enumeradas previamente, el servicio del Servidor de failover/Failover Recording Server establece conexiones salientes a las grabadoras normales, cámaras y para el Envío automático de vídeo.

Log Server servicio

Número de puerto	Protocolo	Proceso	Conexiones desde...	Objetivo
22337	HTTP	Log Server servicio	Todos los componentes de XProtect excepto Management Client y el servidor de grabaciones.	Escribir, leer y configurar el servidor de registros.

Mobile Server servicio

Número de puerto	Protocolo	Proceso	Conexiones desde...	Objetivo
8000	TCP	Mobile Server servicio	Mobile Server Manager icono de la bandeja, solo conexión local.	Aplicación SysTray.
8081	HTTP	Mobile Server servicio	Clientes móviles, clientes web y Management Client.	Enviando flujos de datos; vídeo y audio.
8082	HTTPS	Mobile Server servicio	Clientes móviles y clientes web.	Enviando flujos de datos; vídeo y audio.
40001 - 40099	HTTP	Mobile Server servicio	Servicio del servidor de grabaciones	Mobile Server Push de vídeo. Este rango de puertos está deshabilitado de forma predeterminada.

LPR Server servicio

Número de puerto	Protocolo	Proceso	Conexiones desde...	Objetivo
22334	TCP	LPR Server Servicio	Servidor de evento	Recuperar las matrículas reconocidas y el estado del servidor. Para poder conectarse, el servidor de eventos debe tener instalado el plug-in LPR.
22334	TCP	LPR Server Servicio	LPR Server Manager icono de la bandeja, solo conexión local.	Aplicación SysTray

Milestone Open Network Bridge servicio

Número de puerto	Protocolo	Proceso	Conexiones desde...	Objetivo
580	TCP	Milestone Open Network Bridge Servicio	Clientes de ONVIF	Autenticación y solicitudes para configuración de flujo de vídeo.
554	RTSP	Servicio RTSP	Clientes de ONVIF	Transmisión de vídeo solicitado a clientes de ONVIF.

XProtect DLNA Server servicio

Número de puerto	Protocolo	Proceso	Conexiones desde...	Objetivo
9100	HTTP	DLNA Server Servicio	Dispositivo DLNA	Detección de dispositivos y suministro de configuración de canales DLNA. Solicita flujos de vídeo.
9200	HTTP	DLNA Server Servicio	Dispositivo DLNA	Transmisión de vídeo solicitada a dispositivos de DLNA.

XProtect Screen Recorder servicio

Número de puerto	Protocolo	Proceso	Conexiones desde...	Objetivo
52111	TCP	XProtect Screen Recorder	Recording Server Servicio	Proporciona vídeo desde un monitor. Aparece y actúa del mismo modo que una cámara en el servidor de grabaciones. Puede cargar el número de puerto en Management Client.

XProtect Incident Manager servicio

Número de puerto	Protocolo	Proceso	Conexiones desde...	Objetivo
80	HTTP	IIS	XProtect Smart Client y la Management Client	La finalidad del puerto 80 y del puerto 443 es la misma. Sin embargo, qué puerto utiliza el VMS depende de si usted ha utilizado certificados para proteger la comunicación. • Cuando no se ha protegido la comunicación con certificados, el VMS utiliza el puerto 80. • Si usted ha protegido la comunicación con certificados, el VMS utiliza el puerto 443.
443	HTTPS	IIS		

Componentes del servidor (conexiones salientes)

Management Server servicio

Número de puerto	Protocolo	Conexiones a...	Objetivo
443	HTTPS	El servidor de licencias que alberga el servicio de Gestión de licencias. La comunicación es por medio de https://www.milestonesys.com/OnlineActivation/LicenseManagementService.asmx	Licencias de activación.

Recording Server servicio

Número de puerto	Protocolo	Conexiones a...	Objetivo
80	HTTP	Cámaras, NVR, codificadores Sitios interconectados	Autenticación, configuración y flujos de datos; vídeo y audio. Inicio de sesión
443	HTTPS	Cámaras, NVR, codificadores	Autenticación, configuración y flujos de datos; vídeo y audio.
554	RTSP	Cámaras, NVR, codificadores	Flujos de datos, vídeo y audio.
7563	TCP	Sitios interconectados	Flujos de datos y eventos.
11000	TCP	Servidores de grabación de failover	Agrupando el estado de los servidores de grabación.
40001 – 40099	HTTP	Servicio servidor Mobile	Envío automático de vídeo del servidor móvil. Este rango de puertos está deshabilitado de forma predeterminada.

Failover Server servicio y servicio de Failover Recording Server

Número de puerto	Protocolo	Conexiones a...	Objetivo
11000	TCP	Servidores de grabación de failover	Agrupando el estado de los servidores de grabación.

Event Server servicio

Número de puerto	Protocolo	Conexiones a...	Objetivo
443	HTTPS	Milestone Customer Dashboard vía https://service.milestonesys.com/	Envíe mensajes de estado, eventos y error desde el sistema XProtect a Milestone Customer Dashboard.

Log Server servicio

Número de puerto	Protocolo	Conexiones a...	Objetivo
443	HTTP	Servidor de registro	Reenviando mensajes al servidor de registro.

API Gateway

Número de puerto	Protocolo	Conexiones a...	Objetivo
443	HTTPS	Servidor de gestión	API de RESTful

Cámaras, codificadores y dispositivos de E/S (conexiones entrantes)

Número de puerto	Protocolo	Conexiones desde...	Objetivo
80	TCP	Servidores de grabación y servidores de grabación de failover	Autenticación, configuración y flujos de datos; vídeo y audio.
443	HTTPS	Servidores de grabación y	Autenticación, configuración y

Número de puerto	Protocolo	Conexiones desde...	Objetivo
		servidores de grabación de failover	flujos de datos; vídeo y audio.
554	RTSP	Servidores de grabación y servidores de grabación de failover	Flujos de datos; vídeo y audio.

Cámaras, codificadores y dispositivos de E/S (conexiones salientes)

Número de puerto	Protocolo	Conexiones a...	Objetivo
25	SMTP	Servidores de grabación y servidores de grabación de failover	Enviando notificaciones de eventos (obsoleto).
5432	TCP	Servidores de grabación y servidores de grabación de failover	Enviando notificaciones de eventos. El puerto está deshabilitado de forma predeterminada.
22337	HTTP	Servidor de registro	Reenviando mensajes al servidor de registro.

Solo unos pocos modelos de cámara son capaces de establecer conexiones salientes.

Componentes del cliente (conexiones salientes)

XProtect Smart Client, XProtect Management Client, servidor de XProtect Mobile

Número de puerto	Protocolo	Conexiones a...	Objetivo
80	HTTP	Management Server servicio	Autenticación
443	HTTPS	Management Server servicio	Autenticación de usuarios básicos cuando la encriptación está habilitada.
443	HTTPS	Milestone Systems A/S (doc.milestonesys.com en 52.178.114.226)	Management Client y Smart Client ocasionalmente comprueban si la ayuda en línea está disponible accediendo a la URL de la ayuda.
7563	TCP	Recording Server servicio	Recuperando flujos de vídeo y audio, comandos de PTZ.
22331	TCP	Event Server servicio	Alarmas.

XProtect Web Client, cliente de XProtect Mobile

Número de puerto	Protocolo	Conexiones a...	Objetivo
8081	HTTP	Servidor XProtect Mobile	Recuperando flujos de vídeo y audio.
8082	HTTPS	Servidor XProtect Mobile	Recuperando flujos de vídeo y audio.

API Gateway

Número de puerto	Protocolo	Conexiones a...	Objetivo
80	HTTP	Management Server	API de RESTful
443	HTTPS	Management Server	API de RESTful

Grupos de aplicaciones

El VMS contiene grupos de aplicaciones estándar como.NET v4.5, .NET v4.5 Classic y DefaultAppPool. Los grupos de aplicaciones disponibles en su sistema aparecen en el Administrador de Servicios de Información de Internet (IIS). Además de los grupos de aplicaciones estándar mencionados anteriormente, se entrega un conjunto de grupos de aplicaciones VideoOS con el Milestone XProtect VMS.

Grupos de aplicaciones en Milestone XProtect

En la siguiente tabla puede obtener una descripción general de los grupos de aplicaciones VideoOS que se entregan con Milestone XProtect.

Nombre	Identidad	Objetivo
.NET v4.5	ApplicationPoolId	Característica estándar IIS
.NET v4.5 Classic	ApplicationPoolId	Característica estándar IIS
DefaultAppPool	ApplicationPoolId	Característica estándar IIS
VideoOS ApiGateway	NetworkService	Aloja la pasarela API XProtect, que es la futura API pública y la pasarela al VMS.
VideoOS Classic	NetworkService	Aloja componentes heredados, como la ayuda local, principalmente para cumplir con la compatibilidad con versiones anteriores.
VideoOS IDP	NetworkService	Aloja la API Identity Provider. El Identity Provider crea, mantiene y gestiona la información de identidad de los usuarios básicos y proporciona servicios de autenticación y registro para aplicaciones o servicios de confianza.
VideoOS IM	NetworkService	Aloja la API XProtect Incident Manager. Los documentos XProtect Incident Manager producen incidentes y los combinan con evidencia de secuencia (vídeo y, potencialmente, audio) de sus VMS XProtect.

Trabajar con grupos de aplicaciones

En la página **Grupos de aplicaciones** de la ventana **Servicios de información de Internet (IIS)** puede agregar grupos de aplicaciones o establecer valores predeterminados del grupo de aplicaciones y puede ver las aplicaciones alojadas por cada grupo de aplicaciones.

Abra la página Grupos de aplicaciones

1. En el menú **Inicio** Windows, abra el **Administrador de Servicios de Información de Internet (IIS)**.
2. En el panel **Conexiones**, haga clic en el nombre de su entorno y, a continuación, haga clic en **Grupos de aplicaciones**.
3. En **Acciones**, haga clic en **Agregar grupo de aplicaciones** o en **Establecer valores predeterminados de grupo de aplicaciones** para realizar cualquiera de estas tareas.
4. Seleccione un grupo de aplicaciones en la página **Grupos de aplicaciones** para mostrar más opciones en **Acciones** para cada grupo de aplicaciones.

Comparación de productos

XProtect VMS incluye los siguientes productos:

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

Vea la lista completa de características, que está disponible en la página de descripción del producto en el sitio web Milestone (https://www.milestonesys.com/solutions/platform/product-index/).

Licencias

Licencias (explicación)

Gratis XProtect Essential+

Si ha instalado XProtect Essential+, puede ejecutar el sistema y ocho licencias de dispositivos de forma gratuita. La activación automática de la licencia está habilitada, y el hardware se activará a medida que lo añada al sistema.

Solo cuando se actualiza a un producto XProtect más avanzado y necesita cambiar su SLC (Código de Licencia de Software) (consulte Cambiar el código de licencia del software en la página 127), el resto de este tema y los otros temas relacionados con las licencias en esta documentación podrían ser relevantes para usted.

Licencias para productos VMS XProtect (excepto XProtect Essential+)

Fichero de licencias de software y SLC

Cuando adquiera su software y licencias, recibirá:

- Una confirmación de pedido y un archivo de licencia de software nombrado como su SLC (código de licencia de software) y con la extensión ".lic", por correo electrónico;
- Y cobertura de Milestone Care.

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

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

El archivo de licencia de software contiene toda la información sobre los productos VMS adquiridos, los productos complementarios y las licencias. Milestone recomienda que guarde la información sobre su SLC y una copia de su archivo de licencia de software en un lugar seguro para su uso posterior. También puede ver su SLC en la ventana de **Información de licencia** en Management Client. Puede abrir la ventana de **Información de licencia** en el **Panel de navegación del sitio**-> nodo **Básico** -> **Información de licencia**. Es posible que necesite el archivo de licencia de software o su SLC cuando, por ejemplo, cree una cuenta de usuario de My Milestone, cuando contacte con su distribuidor para recibir asistencia técnica o cuando tenga que realizar cambios en su sistema.

Proceso general de instalación y concesión de licencias

Para empezar, descargue el software desde nuestro sitio web (https://www.milestonesys.com/downloads/). Durante la instalación (consulte Instalar un nuevo sistema XProtect en la página 151) del software, se le pedirá que proporcione el archivo de licencia del software. No puede completar la instalación sin un archivo de

licencia de software.

Una vez que la instalación se haya completado y haya añadido algunas cámaras, debe activar sus licencias (consulte Activación de licencia (explicación) en la página 119). Puede activar sus licencias desde la ventana **Información de licencia** en Management Client. Aquí también puede ver un resumen de sus licencias para todas las instalaciones en el mismo SLC. Puede abrir la ventana de **Información de licencia** en el **Panel de navegación del sitio**-> nodo **Básico** -> **Información de licencia**.

Tipos de licencia

Hay varios tipos de licencia en el sistema de licencias de XProtect.

Licencias básicas

Como mínimo, tiene una licencia base para uno de los productos VMS de XProtect. También puede tener una o más licencias base para productos add-on para XProtect.

Licencias de dispositivo

Como mínimo, tiene varias licencias de dispositivos. Por lo general, necesita una licencia de dispositivo por cada dispositivo de hardware con una cámara que se quiera añadir al sistema. Pero esto puede variar de un dispositivo de hardware a otro y dependiendo de que el dispositivo de hardware sea un dispositivo de hardware soportado o no de Milestone. Si desea más información, consulte Dispositivos de hardware compatibles en la página 118 y Dispositivos de hardware no compatibles en la página 119.

Si desea utilizar la función push de vídeo en XProtect Mobile, también necesita una licencia de dispositivo por cada dispositivo móvil o tableta que pueda enviar vídeo push a su sistema.

No necesita licencias para altavoces, micrófonos, o dispositivos de entrada y salida que estén conectados a sus cámaras.

Dispositivos de hardware compatibles

Por lo general, necesita una licencia de dispositivo por cada dispositivo de hardware con una cámara que se quiera añadir al sistema. Pero algunos dispositivos de hardware compatibles requieren más de una licencia de dispositivo. Puede ver cuántas licencias de dispositivo requieren sus dispositivos de hardware, en la lista de hardware compatible en la página web de Milestone (https://www.milestonesys.com/support/tools-and-references/supported-devices/).

Para los codificadores de vídeo de hasta 16 canales, sólo se necesita una licencia de dispositivo por dirección IP de codificador de vídeo. Un decodificador de vídeo puede tener una o varias direcciones IP.

Sin embargo, si el codificador de vídeo tiene más de 16 canales, se requiere una licencia de dispositivo por cada cámara activada en el codificador de vídeo, también para las primeras 16 cámaras activadas.

Dispositivos de hardware no compatibles

Un dispositivo de hardware no compatible requiere una licencia de dispositivo por cada cámara activada que utilice un canal de vídeo.

Los dispositivos de hardware no compatibles no aparecen en la lista de hardware compatible en el sitio web de Milestone (https://www.milestonesys.com/support/tools-and-references/supported-devices/).

Licencias de cámara para Milestone Interconnect™

Para ejecutar Milestone Interconnect, necesita Milestone Interconnect licencias de cámaras en su sitio central para ver vídeo de los dispositivos de hardware en sitios remotos. El número de Milestone Interconnect licencias de cámara necesarias depende del número de dispositivos de hardware en los sitios remotos de los que se desea recibir datos. Únicamente XProtect Corporate puede desempeñar la función de ubicación central.

Licencias de productos add-on

La mayoría de los productos add-on de XProtect requieren tipos de licencias adicionales. El archivo de licencia de software también incluye información sobre sus licencias para productos add-on. Algunos productos add-on poseen sus propios archivos de licencia de software independientes.

Activación de licencia (explicación)

Su SLC debe estar registrado antes de la instalación (consulte Registrar el código de licencia de software en la página 148). Sus diferentes licencias conectadas con sus SLC deben estar activadas para que el VMS XProtect instalado y los productos complementarios funcionen y los dispositivos de hardware individuales puedan enviar datos al sistema. Para ver un resumen de todos los tipos de licencia de XProtect, consulte Tipos de licencia en la página 118.

Hay varias formas de activar las licencias. Todos ellos están disponibles en la ventana de **Información de licencia**. La mejor forma de activación depende de las políticas de su organización y de si su servidor de gestión tiene acceso a Internet o no. Para saber cómo activar las licencias, consulte Activar sus licencias en la página 124.

Después de la activación inicial de la licencia de su VMS de XProtect, no tiene que activar las licencias de los dispositivos cada vez que añada un dispositivo de hardware con una cámara debido a las flexibilidades incorporadas al sistema de licencias de XProtect. Para obtener más información sobre estas flexibilidades, consulte Periodo de gracia para la activación de la licencia (explicación) en la página 120 y Cambios en el dispositivo sin activación (explicación) en la página 120.

Activación de licencia automática (explicación)

Para facilitar el mantenimiento y la flexibilidad, y cuando las políticas de su organización lo permitan, Milestone recomienda que habilite la activación automática de licencias. La activación automática de la licencia requiere que el servidor de gestión esté en línea. Para saber cómo habilitar la activación automática de la licencia, consulte Activar la activación automática de licencia en la página 124.

Ventajas de habilitar la activación automática de licencias

- El sistema activa sus dispositivos de hardware unos minutos después de que usted haya añadido, eliminado o sustituido dispositivos de hardware o haya realizado otros cambios que afecten al uso de sus licencias. Por lo tanto, solo en raras ocasiones deberá iniciar manualmente la activación de una licencia. Consulte las pocas excepciones en Cuando la activación manual de la licencia sigue siendo necesaria en la página 120.
- El número utilizado de cambios de dispositivo sin activación es siempre cero.
- No hay dispositivos de hardware dentro de un período de gracia y con riesgo de caducidad.
- Si una de sus licencias básicas caduca en un periodo de 14 días, el sistema XProtect también, como precaución adicional, intentará activar automáticamente sus licencias cada noche.

Cuando la activación manual de la licencia sigue siendo necesaria

Si realiza los siguientes cambios en su sistema, se requiere la activación manual de la licencia.

- Comprar licencias adicionales (consulte Obtener licencias adicionales en la página 126)
- Actualizar a una versión más reciente o a un sistema VMS más avanzado (consulte Requisitos de actualización en la página 386)
- Comprar o renovar una suscripción de Milestone Care
- Recibir la autorización para realizar más cambios en el dispositivo sin necesidad de activarlo (consulte Cambios en el dispositivo sin activación (explicación) en la página 120)

Periodo de gracia para la activación de la licencia (explicación)

Cuando haya instalado su VMS y haya añadido dispositivos (dispositivos de hardware, cámaras Milestone Interconnect o licencias de puerta), los dispositivos funcionan en un periodo de gracia de 30 días si ha decidido no habilitar la activación automática de licencias. Antes de que finalice el periodo de gracia de 30 días y si no le quedan más cambios de dispositivos sin activar, debe activar sus licencias, o sus dispositivos dejarán de enviar vídeo a su sistema de vigilancia.

Cambios en el dispositivo sin activación (explicación)

La funcionalidad de los cambios de dispositivo sin activación da flexibilidad incorporada al sistema de licencias XProtect. Por tanto, aunque haya decidido activar las licencias manualmente, no tiene por qué activarlas cada vez que añada o elimine dispositivos de hardware.

El número de cambios de dispositivo sin activación difiere de una instalación a otra y se calcula en función de varias variables. Para obtener una descripción detallada, consulte Cálculo del número disponible de cambios de dispositivo sin activación (explicación) en la página 121.

Un año después de la última activación de la licencia, el número de cambios de dispositivo utilizados sin activación se pone automáticamente a cero. Una vez que el reinicio tiene lugar, puede seguir añadiendo y sustituyendo dispositivos de hardware sin activar las licencias.

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

Debe explicar por qué cree que tiene derecho a un mayor número de cambios de dispositivo sin activación. Milestone decide cada solicitud de forma individual. En caso de que se le conceda un número mayor de cambios de dispositivo sin activación, deberá activar sus licencias para registrar el número mayor en su sistema XProtect.

Cálculo del número disponible de cambios de dispositivo sin activación (explicación)

El número disponible de cambios de dispositivo sin activación se calcula en base a tres variables. Si tiene varias instalaciones del software Milestone, las variables se aplican a cada una de ellas 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 dispositivos sin activación
- **Cmax** que es un valor máximo fijo del número de cambios de dispositivos sin activación

El número de cambios de dispositivo sin activación nunca puede ser inferior al valor **Cmin** ni superior al valor **Cmax**. El valor calculado en base a la variable **C%** cambia según el número de dispositivos activados que tenga en cada instalación de su sistema. Los dispositivos añadidos con cambios de dispositivo sin activación no se cuentan como activados por la variable **C%**.

Milestone define los valores de las tres variables y los valores están sujetos a cambios sin previo aviso. Los valores de las variables difieren según el producto.

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

Compra 100 licencias de dispositivos. A continuación, se añaden 100 cámaras al sistema. A menos que haya habilitado la activación automática de la licencia, el número de cambios de dispositivo sin activación sigue siendo cero. Activa sus licencias y ahora tiene 15 cambios de dispositivo sin activación.

Compra 100 licencias de dispositivos. Después, añade 100 cámaras al sistema y activa las licencias. Su número de cambios de dispositivo sin activación es ahora de 15. A continuación, decide eliminar un dispositivo de hardware del sistema. Ahora tiene 99 dispositivos activados y el número de cambios de dispositivo sin activación ha bajado a 14.

Compra 1000 licencias de dispositivos. Después, añade 1000 cámaras y activa las licencias. Sus cambios de dispositivo sin activación son ahora 100. Según la variable **C%**,ahora debería haber tenido 150 cambios de dispositivo sin activación, pero la variable **Cmax** solo le permite tener 100 cambios de dispositivo sin activación.

Compra 10 licencias de dispositivos. Después, añade 10 cámaras al sistema y activa las licencias. Su número de cambios de dispositivo sin activación es ahora de 10 debido a la variable **Cmin**. Si el número se calculara solo en base a la variable **C%**, solo habría tenido 1 (15% de10 = 1,5 redondeado a 1).

Compra 115 licencias de dispositivos. Después, añade 100 cámaras al sistema y activa las licencias. Sus cambios de dispositivo sin activación son ahora 15. Añade otras 15 cámaras sin activarlas, utilizando 15 de los 15 cambios de dispositivo sin activación. Ahora elimina 50 de las cámaras del sistema y el número de cambios de dispositivo sin activación baja a 7. Esto significa que 8 de las cámaras añadidas anteriormente dentro de los 15 cambios de dispositivo sin activación entran en un periodo de gracia. Ahora añade 50 cámaras nuevas. Debido a que usted activó 100 cámaras en el sistema la última vez que activó las licencias, el número de cambios de dispositivo sin activación vuelve a ser 15 y las 8 cámaras, que fueron movidas a un período de gracia, regresan como cambios de dispositivo sin activación. Las 50 nuevas cámaras entran en un periodo de gracia.

Milestone Care™ (explicación)

Milestone Care es el nombre del programa completo de servicio y asistencia para los productos XProtect durante toda su vida útil.

Milestone Care le da acceso a diferentes tipos de material de autoayuda como artículos de Knowledge Base (Base de conocimiento), guías y tutoriales en nuestro sitio web de soporte (https://www.milestonesys.com/support/).

Para obtener beneficios adicionales, puede comprar más suscripciones anticipadas de Milestone Care.

Milestone Care Plus

Si tiene una suscripción Milestone Care Plus, también tiene acceso a actualizaciones gratuitas de su producto XProtect VMS actual y puede actualizar a productos XProtect VMS más avanzados a un precio ventajoso. Milestone Care Plus también ofrece funcionalidad adicional:

- El servicio Panel de usuario
- La característica Conexión inteligente
- La funcionalidad completa de notificación push

Milestone Care Premium

Si tiene una suscripción Milestone Care Premium, también puede ponerse en contacto con el servicio de asistencia Milestone directamente. Recuerde incluir la información sobre su ID Milestone Care cuando se ponga en contacto con el servicio de asistencia de Milestone.

Vencimiento, renovación y compra de suscripciones Milestone Care avanzadas

La fecha de caducidad de los tipos de suscripción de Milestone Care Plus y Milestone Care Premium más avanzados son visibles en la ventana de **información de la licencia** en la tabla de **productos instalados**. Consulte Productos instalados en la página 129.

Si decide comprar o renovar una suscripción de Milestone Care después de haber instalado su sistema, deberá activar manualmente sus licencias para que aparezca la información correcta de Milestone Care. Consulte Activar licencias en línea en la página 125 o Activar licencias fuera de línea en la página 125.

Licencias y sustitución de hardware (explicación)

Si una cámara del sistema se estropea o si, por otros motivos, desea sustituirla por una nueva, existen algunas prácticas recomendadas sobre cómo debe hacerse.

Si se elimina una cámara de un servidor de grabación, se libera una licencia de dispositivo, pero también se pierde el acceso completo a todas las bases de datos (cámaras, micrófonos, entradas, salidas) y la configuración de la cámara antigua. Para mantener el acceso a las bases de datos de la antigua cámara y reutilizar sus ajustes al sustituirla por una nueva, utilice la opción correspondiente que aparece a continuación.

Sustituir la cámara por otra similar

Si sustituye una cámara por otra similar (fabricante, marca y modelo), y si le da a la nueva cámara la misma dirección IP que la antigua, mantendrá el acceso completo a todas las bases de datos de la antigua cámara. La nueva cámara sigue utilizando las mismas bases de datos y ajustes que la antigua. En este caso, se mueve el cable de red de la cámara antigua a la nueva sin cambiar ninguna configuración en Management Client.

Sustituir la cámara por otra diferente

Si sustituye una cámara por otra diferente (fabricante, marca y modelo), debe utilizar el asistente **Sustituir hardware** (consulte Sustituir el hardware en la página 356) para asignar todas las bases de datos relevantes de la cámara antigua a la nueva y reutilizar los ajustes de la cámara antigua.

Activación de la licencia tras la sustitución del hardware

Si ha habilitado la activación automática de la licencia (consulte Activar la activación automática de licencia en la página 124), la nueva cámara se activará automáticamente.

Si la activación automática de las licencias está desactivada, y si se han utilizado todos los cambios de dispositivo disponibles sin activación (consulte Cambios en el dispositivo sin activación (explicación) en la página 120), deberá activar manualmente sus licencias. Para obtener más información sobre la activación manual de licencias, consulte Activar licencias en línea en la página 125 o Activar licencias fuera de línea en la página 125.

Obtener una visión general de sus licencias

Hay muchas razones por las que le gustaría obtener una visión general de sus SLC y su número de licencias adquiridas y sus estados. Estas son unas pocas:

- ¿Quiere añadir uno o varios dispositivos de hardware nuevos, pero tiene licencias de dispositivos sin usar o tiene que comprar otras nuevas?
- ¿El periodo de gracia de algunos de sus dispositivos de hardware termina pronto? A continuación, debe activarlos antes de que dejen de enviar datos al VMS.

- Ya sabe, por contactos anteriores con el servicio de asistencia, que necesitan información sobre su SLC y su ID Milestone Care para poder ayudarle. ¿Pero cuáles son?
- Tiene muchas instalaciones de XProtect y utiliza el mismo SLC para todas las instalaciones, pero ¿dónde se utilizan las licencias y cuáles son sus estados?

Puede encontrar toda la información anterior y más en la ventana de **Información de licencia**.

Puede abrir la ventana de **Información de licencia** en el **Panel de navegación del sitio**-> nodo **Básico** -> **Información de licencia**.

Para saber más sobre las distintas informaciones y funciones disponibles en la ventana de **Información sobre licencia**, consulte Ventana de información de la licencia en la página 128.

Activar sus licencias

Hay varias formas de activar las licencias. Todos ellos están disponibles en la ventana de **Información de licencia**. La mejor forma de activación depende de las políticas de su organización y de si su servidor de gestión tiene acceso a Internet o no.

Puede abrir la ventana de **Información de licencia** en el **Panel de navegación del sitio**-> nodo **Básico** -> **Información de licencia**.

Para saber más sobre las distintas informaciones y funciones disponibles en la ventana de **Información sobre licencia**, consulte Ventana de información de la licencia en la página 128.

Activar la activación automática de licencia

Para facilitar el mantenimiento y la flexibilidad, y cuando las políticas de su organización lo permitan, Milestone recomienda que habilite la activación automática de licencias. La activación automática de la licencia requiere que el servidor de gestión esté en línea.

Si desea conocer todas las ventajas de habilitar la activación automática de la licencia, consulte Activación de licencia automática (explicación) en la página 119.

1. En el panel de **Navegación del sitio** -> nodo **Básico** -> **Información sobre la licencia**, seleccione **Activar la activación automática de licencia**.
2. Introduzca el nombre de usuario y la contraseña que desea utilizar con la activación automática de la licencia:
   - Si ya es usuario, introduzca su nombre de usuario y contraseña para iniciar sesión en el sistema de registro del software
   - Si es un nuevo usuario, haga clic en el enlace **Crear nuevo usuario** para crear una nueva cuenta de usuario y siga el procedimiento de registro. Si aún no ha registrado su código de licencia de software (SLC), debe hacerlo

   Las credenciales se guardan en un archivo en el servidor de gestión.
3. Haga clic en **Aceptar**.

Si más adelante quiere cambiar su nombre de usuario y/o la contraseña para la activación automática, haga clic en el enlace **Editar credenciales de activación**.

Deshabilitar la activación automática de licencia

Si no está permitido utilizar la activación automática de licencias en su organización o simplemente ha cambiado de opinión, puede desactivar la activación automática de licencias.

La forma de deshabilitarla depende de si más adelante piensa volver a utilizar la activación automática de licencias o no.

Deshabilitar pero conservar la contraseña para su uso posterior:

1. En el panel de **Navegación del sitio** -> nodo **Básico** -> **Información sobre la licencia**, desactive **Habilitar la activación automática de la licencia**. El nombre de usuario y la contraseña se siguen guardando en el servidor de gestión.

Deshabilitar y eliminar la contraseña:

1. En el panel de **Navegación del sitio** -> nodo **Básico** -> **Información sobre la licencia**, haga clic en **Editar credenciales de activación**.
2. Haga clic en **Eliminar contraseña**.
3. Confirme que desea eliminar el nombre de usuario y la contraseña del servidor de gestión.

Activar licencias en línea

Si el servidor de gestión tiene acceso a Internet pero prefiere iniciar manualmente el proceso de activación, ésta es la opción de activación de licencias más sencilla que tiene.

1. En el panel de **Navegación del sitio** -> nodo **Básico** -> **Información sobre la licencia**, seleccione **Activar licencia manualmente** y a continuación **En línea**.
2. Se abre el cuadro de diálogo **Activar en línea**:
   - Si ya es usuario, introduzca su nombre de usuario y contraseña
   - Si es un nuevo usuario, 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 **Aceptar**.

Si recibe un mensaje de error durante la activación en línea, siga las instrucciones que aparecen en la pantalla para resolver el problema o póngase en contacto con el servicio de asistencia de Milestone.

Activar licencias fuera de línea

Si su organización no permite que el servidor de gestión tenga acceso a Internet, deberá activar las licencias manualmente y sin conexión.

1. En el panel de **Navegación del Sitio** -> nodo **Conceptos básicos** -> **Información de licencia**, seleccione **Activar licencia manualmente** > **Fuera de línea** > **Exportar licencia para activación** exportar un archivo de solicitud de licencia (.lrq) con información sobre sus dispositivos de hardware añadidos y otros elementos que requieren una licencia.
2. El archivo de solicitud de licencia (.lrq) recibe automáticamente el mismo nombre que su SLC. Si tiene varios sitios, recuerde cambiar el nombre de los archivos para poder identificar fácilmente qué archivo pertenece a cada sitio.
3. Copie el archivo de solicitud de licencia en un ordenador con acceso a Internet e inicie sesión en nuestro sitio web (https://online.milestonesys.com/) para obtener el archivo de licencia de software activado (.lic).
4. Copie el archivo .lic que reciba en su ordenador con Management Client. El archivo ha recibido el mismo nombre que su archivo de solicitud de licencia.
5. En el panel de **Navegación del sitio** -> nodo **Básico** -> **Información de licencia**, seleccione **Activar licencia fuera de línea** > **Importar licencia activada**, y luego seleccione el archivo de licencia de software activado para importarlo y así activar sus licencias.
6. Haga clic en **Finalizar** para finalizar el proceso de activación.

Activar licencias después del periodo de gracia

Si ha decidido utilizar la activación manual de la licencia y ha olvidado activar una licencia dentro del periodo de gracia (dispositivo de hardware, cámara Milestone Interconnect, licencias de puerta u otros), el dispositivo que utiliza esa licencia deja de estar disponible y no puede enviar datos al sistema de vigilancia

Aunque el periodo de gracia de una licencia haya expirado, la configuración del dispositivo y los ajustes realizados se guardan y se utilizan cuando se activa la licencia.

Para habilitar de nuevo los dispositivos no disponibles, activa las licencias manualmente de la forma que prefieras. Si desea más información, consulte Activar licencias fuera de línea en la página 125 o Activar licencias en línea en la página 125.

Obtener licencias adicionales

Si desea añadir o si ya ha añadido más dispositivos de hardware, sistemas Milestone Interconnect,puertas u otros elementos para los que actualmente tiene licencias, deberá comprar licencias adicionales para habilitarlos para enviar datos a su sistema:

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

Si ha comprado nuevas licencias para su versión del sistema de vigilancia existente:

- Simplemente active sus licencias manualmente para tener acceso a las nuevas licencias. Si desea más información, consulte Activar licencias en línea en la página 125 o Activar licencias fuera de línea en la página 125.

Si ha comprado nuevas licencias y una versión actualizada del sistema de vigilancia:

- Recibirá un archivo de licencia de software actualizado (**.lic**) (consulte Licencias (explicación) en la página 117) con las nuevas licencias y la nueva versión. Debe utilizar el nuevo archivo de licencia de software durante la instalación de la nueva versión. Si desea más información, consulte Requisitos de actualización en la página 386

Cambiar el código de licencia del software

Si realiza una instalación con un Código de Licencia de Software (SLC) temporal o si ha actualizado a un producto más avanzado XProtect, puede cambiar su SLC por un SLC permanente o más avanzado. Puede cambiar su SLC sin necesidad de realizar ninguna acción de desinstalación o reinstalación cuando haya recibido su nuevo archivo de licencia de software.

Puede hacerlo localmente en el servidor de gestión o remotamente desde Management Client.

Desde el icono de la bandeja del servidor de gestión

1. En el servidor de gestión, vaya al 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 de software guardado para este fin. Una vez hecho esto, la ubicación del archivo de licencia de software seleccionado se añade justo debajo del botón **Importar licencia**.
5. Haga clic en **Aceptar** y ya está a punto para registrar el SLC. Consulte Registrar el código de licencia de software en la página 148.

Desde Management Client

1. Copie el archivo .lic que reciba en su ordenador con Management Client.
2. En el panel de **Navegación del sitio** -> nodo **Básico** -> **Información de licencia**, seleccione **Activar licencia fuera de línea** > **Importar licencia activada**, y luego seleccione el archivo de licencia de software activado para importarlo.
3. Cuando se abra, acepte que el archivo de licencia de software es diferente del que se está utilizando

actualmente.

4. Ahora está en condiciones de registrar el SLC. Consulte Registrar el código de licencia de software en la página 148.

> El archivo de licencia del software solo se importa y se modifica, pero no se activa. Recuerde activar su licencia. Si desea más información, consulte Activar sus licencias en la página 124.

> Cuando se ejecuta XProtect Essential+, solo se puede cambiar la licencia desde el icono de la bandeja del servidor de gestión. No es posible cambiar la licencia de Management Client.

Ventana de información de la licencia

En la ventana de **Información de licencia**, puede llevar un registro de todas las licencias que comparten el mismo archivo de licencia de software tanto en este sitio como en todos los demás sitios, sus suscripciones de Milestone Care y decidir cómo quiere activar sus licencias.

Puede abrir la ventana de **Información de licencia** en el **Panel de navegación del sitio**-> nodo **Básico** -> **Información de licencia**.

Si quiere tener una comprensión general de cómo funciona el sistema de licencias XProtect, consulte Licencias (explicación) en la página 117.

Licencia concedida a

Esta área de la ventana de **Información de licencia**, enumera los datos de contacto del propietario de la licencia que se introdujo durante el registro del software.

Si no puede ver el área **Licencia concedida a**, haga clic en el botón **Actualizar** en la esquina inferior derecha de la ventana.

Haga clic en **Editar detalles** para editar la información del propietario de la licencia. Haga clic en **Acuerdo de licencia de usuario final** para ver el acuerdo de licencia de usuario final que aceptó antes de la instalación.

Milestone Care

Aquí puede ver información sobre su suscripción actual de Milestone Care™. Las fechas de caducidad de sus suscripciones se muestran en la tabla de **Productos instalados** que aparece a continuación.

Para obtener más información sobre Milestone Care, utilice los enlaces o consulte Milestone Care™ (explicación) en la página 122.

Productos instalados

Muestra la siguiente información sobre todas las licencias base instaladas para XProtect VMS y los productos complementarios que comparten el mismo archivo de licencia de software:

- Productos y versiones
- El código de licencia del software de los productos (SLC)
- La fecha de caducidad de su SLC. Normalmente, no restringida.
- La fecha de vencimiento de su suscripción de Milestone Care Plus
- La fecha de vencimiento de su suscripción de Milestone Care Premium

Installed Products

Product Version	Software License Code	Expiration Date	Milestone Care Plus	Milestone Care Premium
XProtect Corporate 20 R	M01-C01-211-01-	Unlimited	16-11-20	16-11-20
Milestone XProtect Smart Wall	M01-P03-100-01-	Unlimited	Unlimited	
Milestone XProtect Access	M01-P01-011-01-	Unlimited	Unlimited	
Milestone XProtect Transact	M01-P08-100-01-	Unlimited	Unlimited	

Descripción de la licencia - Todos los sitios

Muestra el número de licencias de dispositivo activadas y otras licencias en su archivo de licencia de software y el número total de licencias disponibles en su sistema. Aquí puede ver fácilmente si todavía puede hacer crecer su sistema sin comprar licencias adicionales.

Para obtener una visión detallada del estado de sus licencias activadas en otros sitios, haga clic en el enlace **Detalles de la licencia - Todos los sitios**. Consulte la sección **Detalles de la licencia - Sitio actual** para conocer la información disponible que se muestra.

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

License Type	Activated
Device Licenses	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 complementarios, puede ver detalles adicionales sobre éstos en los nodos específicos de los productos complementarios en el panel de **Navegación del sitio**.

Detalles de la licencia: sitio actual

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

También puede ver el número de cambios de dispositivo utilizados sin activación (consulte Cambios en el dispositivo sin activación (explicación) en la página 120) y cuántos tiene disponibles al año en la columna **Cambios sin activación.**.

Si tiene licencias que aún no ha activado y que, por tanto, están en periodo de gracia, éstas aparecen en la columna **En periodo de gracia**. La fecha de caducidad de la primera licencia que expira, aparece en rojo debajo de la tabla.

Si se olvida de activar las licencias antes de que expire el periodo de gracia, dejarán de enviar vídeo al sistema. Estas licencias se muestran en la columna **Periodo de gracia caducado**. Si desea más información, consulte Activar licencias después del periodo de gracia en la página 126.

Si ha utilizado más licencias de las que tiene disponibles, éstas aparecen en la columna **Sin licencia** y no pueden ser utilizadas en su sistema. Si desea más información, consulte Obtener licencias adicionales en la página 126.

Si tiene licencias en periodo de gracia, con un periodo de gracia caducado o sin licencia, un mensaje le recordará cada vez que inicie sesión en su Management Client.

License Details - Current Site: [redacted]

License Type	Activated	Changes without activation	In Grace Period	Grace Period Expired	Without License
Device Licenses	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

Si tiene dispositivos de hardware que utilizan más de una licencia, aparece un enlace **Haga clic aquí para abrir el informe completo de la licencia del dispositivo** debajo de la tabla **Detalles de la licencia - Sitio actual**. Al hacer clic en el enlace, puede ver cuántas licencias de dispositivo requiere cada uno de estos dispositivos de hardware.

Los dispositivos de hardware sin licencia se identifican con un signo de exclamación en el Management Client. El signo de exclamación también se utiliza para otros fines. Coloque el ratón sobre el signo de exclamación para ver el propósito.

Funciones de activación de licencias

Debajo las tres tablas son:

- Una casilla para habilitar la activación automática de la licencia y un enlace para editar las credenciales del usuario para la activación automática. Si desea más información, consulte Activación de licencia automática (explicación) en la página 119 y Activar la activación automática de licencia en la página 124. Si la activación automática ha fallado, aparecerá un mensaje de error en rojo. Para obtener más información, haga clic en el enlace **Detalles**.
  Algunas licencias , como XProtect Essential+, se instalan con la activación automática de la licencia habilitada, y no es posible desactivarla.
- Una lista desplegable para activar manualmente las licencias en línea o fuera de línea. Si desea más información, consulte Activar licencias en línea en la página 125 y Activar licencias fuera de línea en la página 125.
- En la esquina inferior derecha de la ventana, puede ver cuándo se activaron sus licencias por última vez (automática o manualmente) y cuándo se actualizó la información en la ventana. Las marcas de tiempo son del servidor y no del ordenador local


Enable automatic license activation
Edit activation credentials...
Activate License Manually...
Online
Offline
Last activated: 17. november 20 15:02:00
Information refreshed: 28. januar 20 11:39:11

Requisitos y consideraciones

Horario de verano (explicación)

El horario de verano (DST) es la práctica de adelantar los relojes para que las tardes tengan más luz solar y las mañanas menos. El uso del horario de verano varía según los países/regiones.

Cuando trabaje con un sistema de vigilancia, que sea intrínsecamente sensible a la hora, es importante que sepa cómo maneja el sistema el horario de verano.

> ⚠ No cambie la configuración del horario de verano cuando se encuentre en el período DST o si tiene grabaciones de un período DST.

Primavera: Cambio de hora estándar a horario de verano

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

Ejemplo:

El reloj se adelanta de las 02:00 horas estándar a las 03:00 horas del horario de verano, y el día tiene 23 horas. En ese caso, no hay datos entre las 02:00 y las 03:00 de la mañana ya que esa hora, para ese día, no existía.

Otoño: Cambiar del horario de verano al horario estándar

Cuando se pasa del horario de verano a la hora estándar en otoño, se retrocede una hora.

Ejemplo:

El reloj se adelanta de las 02:00 horas del horario de verano a las 01:00 horas estándar, y el día tiene 25 horas. Se llega a la 01:59:59 y de inmediato se vuelve a la 01:00:00. Si el sistema no reaccionara, esencialmente volvería a registrar esa hora, por lo que la primera instancia de 01:30 sería sobrescrita por la segunda instancia de 01:30.

Para evitar que este problema ocurra, el sistema archiva el vídeo actual en caso de que la hora del sistema cambie más de cinco minutos. No se puede ver la primera instancia de la hora 01:00 directamente en ningún cliente, pero los datos quedan registrados y a salvo. Puede consultar este vídeo en XProtect Smart Client abriendo directamente la base de datos archivada.

Servidores de tiempo (explicación)

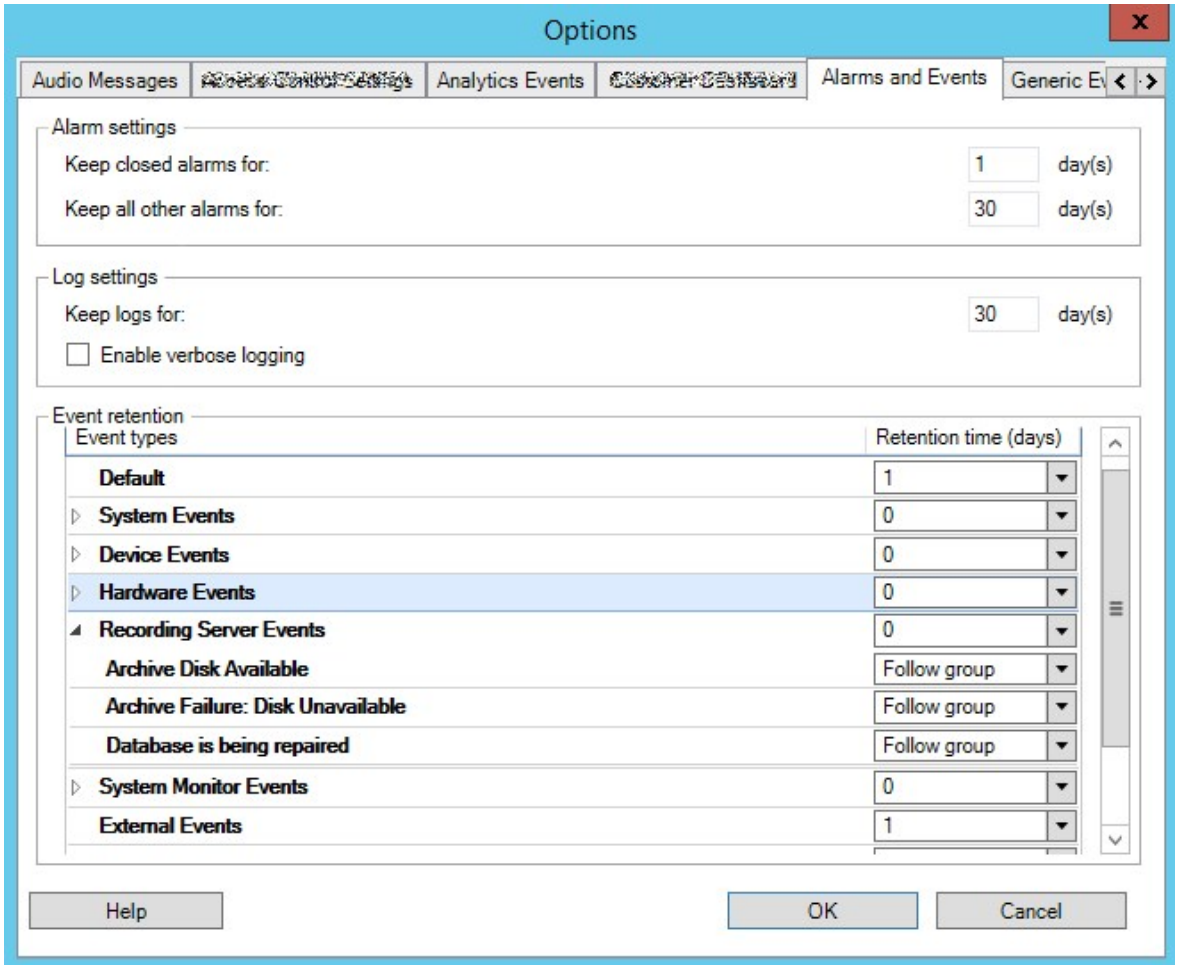
Una vez que el sistema recibe las imágenes, éstas se marcan instantáneamente con la hora. Como las cámaras son unidades separadas que pueden tener dispositivos de temporización distintos, la hora de la cámara y la de su sistema pueden no coincidir completamente. En ocasiones, esto puede dar lugar a confusión. Si sus cámaras son compatibles con las marcas de tiempo, Milestone recomienda sincronizar automáticamente la hora de la cámara y del sistema a través de un servidor de tiempo para una sincronización consistente.

Para obtener información sobre cómo configurar un servidor de tiempo, busque en el sitio web de Microsoft (https://www.microsoft.com/) por **'servidor de tiempo'**, **'servicio de tiempo'**, o términos similares.

Limitar el tamaño de la base de datos

Para evitar que la base de datos SQL (consulte Instalaciones SQL Server y bases de datos (explicación) en la página 33) crezca hasta un tamaño que afecte al rendimiento del sistema, puede especificar durante cuántos días se almacenan en la base de datos los diferentes tipos de eventos y alarmas.

1. Abra el menú **Herramientas**.
2. Hagaclicenlapestaña**Opciones**>**AlarmasyEventos**.



3. Realice los ajustes necesarios. Si desea más información, consulte Pestaña Alarmas y eventos (opciones) en la página 412.

IPv6 y IPv4 (explicación)

Su sistema es compatible con IPv6 y con IPv4. Igual que XProtect Smart Client.

IPv6 es la última versión del Protocolo de Internet (IP). El protocolo de Internet determina el formato y el uso de las direcciones IP. IPv6 coexiste con la versión de IP, IPv4, aún mucho más utilizada. IPv6 se desarrolló para solucionar el agotamiento de direcciones de IPv4. Las direcciones IPv6 tienen una longitud de 128 bits, mientras que las direcciones IPv4 solo tienen 32 bits.

Esto significó que la agenda de direcciones de Internet pasó de 4,3 mil millones de direcciones únicas a 340 undecillones (340 trillones de trillones). Un factor de crecimiento de 79 octillones (billones de billones).

Cada vez más organizaciones están implantando IPv6 en sus redes. Por ejemplo, todas las infraestructuras de las agencias federales de Estados Unidos deben ser compatibles con IPv6. Los ejemplos e ilustraciones de este manual reflejan el uso de IPv4 porque sigue siendo la versión de IP más utilizada. IPv6 funciona igualmente bien con el sistema.

Uso del sistema con IPv6 (explicación)

Las siguientes condiciones se aplican cuando se utiliza el sistema con IPv6:

Servidores

A menudo, los servidores pueden utilizar tanto IPv4 como IPv6. Sin embargo, si un solo servidor del sistema (por ejemplo, un servidor de gestión o un servidor de grabación) requiere una versión IP concreta, todos los demás servidores del sistema deben comunicarse utilizando la misma versión IP.

Ejemplo: Todos los servidores de su sistema, excepto uno, pueden utilizar tanto IPv4 como IPv6. La excepción es un servidor que solo puede utilizar IPv6. Esto significa que todos los servidores deben comunicarse entre sí utilizando IPv6.

Dispositivos

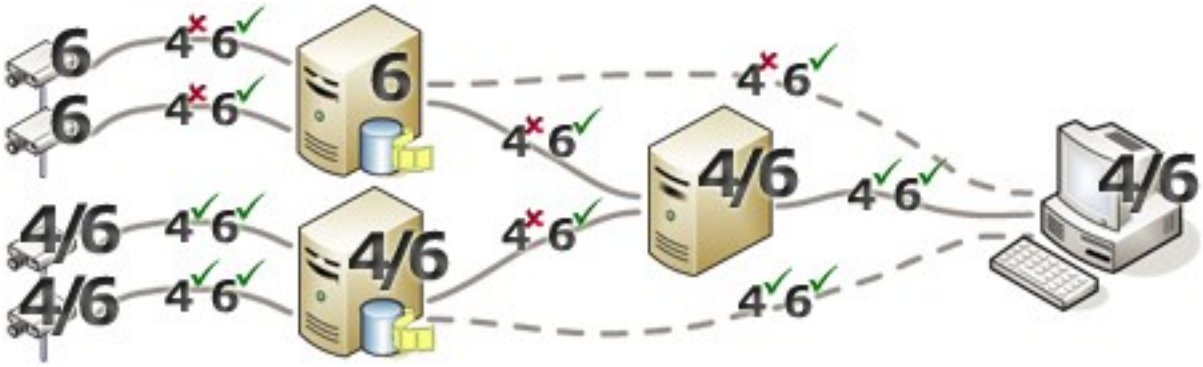
Puede utilizar dispositivos (cámaras, entradas, salidas, micrófonos, altavoces) con una versión IP diferente a la que se utiliza para la comunicación con el servidor, siempre que su equipo de red y los servidores de grabación también soporten la versión IP de los dispositivos. Consulte también la siguiente ilustración.

Clientes

Si su sistema utiliza IPv6, los usuarios deben conectarse con el XProtect Smart Client. El XProtect Smart Client es compatible con IPv6 igual que con IPv4.

Si uno o más servidores de su sistema **solo** pueden utilizar IPv6, los usuarios XProtect Smart Client **deben** utilizar IPv6 para su comunicación con esos servidores. En este contexto, es importante recordar que las instalaciones XProtect Smart Client se conectan técnicamente a un servidor de gestión para la autentificación inicial, y luego a los servidores de grabación necesarios para acceder a las grabaciones.

Sin embargo, no es necesario que los usuarios de XProtect Smart Client estén en una red IPv6, siempre que su equipo de red admita la comunicación entre diferentes versiones de IP y que hayan instalado el protocolo IPv6 en sus ordenadores. Consulte también la ilustración. Para instalar IPv6 en un ordenador cliente, abra un símbolo del sistema, introduzca ***instalar Ipv6***, y pulse **ENTER**.
Ilustración de ejemplo



Ejemplo: Como un servidor del sistema solo puede utilizar IPv6, toda la comunicación con ese servidor debe utilizar IPv6. Sin embargo, ese servidor también determina la versión IP para la comunicación entre todos los demás servidores del sistema.

Escribir direcciones IPv6 (explicación)

Una dirección IPv6 suele escribirse en ocho bloques de cuatro dígitos hexadecimales, con cada bloque separado por dos puntos.

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

Puede acortar las direcciones eliminando los ceros a la izquierda de un bloque. Además, tenga en cuenta que algunos de los bloques de cuatro dígitos pueden estar formados solo por ceros. Si cualquier número de estos bloques 0000 son consecutivos, puede acortar las direcciones sustituyendo los bloques 0000 por dos dos puntos, siempre que solo haya uno de estos dos puntos dobles en la dirección.

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

2001:B80:0000:0000:0000:F80:3FA8:18AB si se eliminan los ceros iniciales, o a

2001:0B80::0F80:3FA8:18AB si se eliminan los bloques 0000, o incluso a

2001:B80::F80:3FA8:18AB si se eliminan los ceros iniciales y los bloques 0000.

Uso de las direcciones IPv6 en las URL

Las direcciones IPv6 contienen dos puntos. No obstante, los dos puntos también se utilizan en otros tipos de sintaxis de direccionamiento de red. Por ejemplo, IPv4 utiliza dos puntos para separar la dirección IP y el número de puerto cuando ambos se utilizan en una URL. IPv6 ha heredado este principio. Por lo tanto, para evitar confusiones, se ponen corchetes 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, por supuesto, puede acortarse 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, por supuesto, puede acortarse a, por ejemplo, *http://[2001:B80::F80:3FA8:18AB]:1234*

Para obtener más información IPv6, consulte, por ejemplo, el sitio web de IANA (https://www.iana.org/numbers/). IANA, la Autoridad de Asignación de Números de Internet, es la organización responsable de la coordinación global del direccionamiento IP.

Servidores virtuales

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

A menudo se prefiere la virtualización para aprovechar mejor los recursos de hardware. Normalmente, los servidores virtuales que se ejecutan en el servidor host de hardware no cargan el servidor virtual hasta un punto excesivo, y a menudo no al mismo tiempo. No obstante, los servidores de grabación registran todas las cámaras y flujos de vídeo. Esto supone una gran carga para la CPU, la memoria, la red y el sistema de almacenamiento. Por ello, cuando se ejecuta en un servidor virtual, la ganancia normal de la virtualización desaparece en gran medida, ya que, en muchos casos, utiliza todos los recursos disponibles.

Si se ejecuta en un entorno virtual, es importante que el host de hardware tenga la misma cantidad de memoria física que la asignada a los servidores virtuales y que el servidor virtual que ejecuta el servidor de grabación tenga asignada suficiente CPU y memoria, lo que no sucede por defecto. Normalmente, el servidor de grabación necesita entre 2 y 4 GB, dependiendo de la configuración. Otro cuello de botella es la asignación del adaptador de red y el rendimiento del disco duro. Tenga en cuenta la posibilidad de asignar un adaptador de red físico en el servidor host del servidor virtual que ejecuta el servidor de grabación. Esto facilita que el adaptador de red no se sobrecargue con el tráfico de otros servidores virtuales. Si el adaptador de red se utiliza para varios servidores virtuales, el tráfico de red podría hacer que el servidor de grabación no recuperara y grabara el número de imágenes configurado.

Múltiples servidores de gestión (clustering) (explicación)

El servidor de gestión puede instalarse en varios servidores dentro de un clúster de servidores. Esto garantiza que el sistema tenga muy poco tiempo de inactividad. Si un servidor del clúster falla, otro servidor del clúster asume automáticamente el trabajo del servidor que ha fallado ejecutando el servidor de gestión.

Solo es posible tener un servidor de gestión activo por configuración de vigilancia, pero se pueden configurar otros servidores de gestión para que se hagan cargo en caso de fallo.

Por defecto, el servicio de Management Server limita el número de veces que se produce un failover a dos en un periodo de seis horas. Si se supera, los servicios de Management Server no son iniciados automáticamente por el servicio de clustering. Este límite puede modificarse para que se adapte mejor a sus necesidades.

Requisitos para el clustering

- Dos máquinas con Microsoft Windows Server 2016 o más reciente. Asegúrese de que:
  - Todos los servidores que desea añadir como nodos del clúster están ejecutando la misma versión de Windows Server
  - Todos los servidores que desea añadir como nodos del clúster están unidos al mismo dominio
  - Tiene acceso a la cuenta de Windows como administrador local

  Acerca de los clústeres en servidores Microsoft Windows, consulte clústeres de failover https://docs.microsoft.com/en-us/windows-server/failover-clustering/create-failover-cluster.
- Una instalación de Microsoft SQL Server

  Ya sea un SQL Server externo y una base de datos instalada **fuera** del clúster de servidores **o** un servicio SQL Server**interno** (en clúster) dentro del clúster de servidores (la creación de un servicio interno SQL Server requiere el uso de la edición Microsoft® SQL Server® Standard o Microsoft® SQL Server® Enterprise, que puede funcionar como clústerSQL Server).

  > Al conectar el servidor de gestión a la base de datos, dependiendo de los ajustes de la contraseña de configuración del sistema, es posible que se le pida que proporcione la contraseña de configuración del sistema actual. Consulte Contraseña de configuración del sistema (explicación) en la página 343.

> Si trabaja en un entorno de clúster de failover, se recomienda poner en pausa el clúster antes de iniciar las tareas en el Server Configurator. Esto se debe a que Server Configurator puede ser necesario detener los servicios mientras se aplican los cambios y el entorno del clúster de failover puede interferir con esta operación.

Proteger las bases de datos de grabación de la corrupción

Las bases de datos de las cámaras pueden corromperse. Existen varias opciones de reparación de bases de datos para resolver dicho problema. pero Milestone recomienda tomar medidas para garantizar que las bases de datos de la cámara no se corrompan.

Fallo del disco duro: proteger las 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 provocar la corrupción de las bases de datos de las cámaras:

- Vibración (asegúrese de que el servidor del sistema de vigilancia y su entorno son estables)
- Calor fuerte (asegúrese de que el servidor tiene una ventilación adecuada)
- Campos magnéticos fuertes (evitar)
- Cortes de energía (asegúrese de utilizar un sistema de alimentación ininterrumpida (SAI))
- Electricidad estática (asegúrese de tener una conexión a tierra si va a manipular un disco duro)
- Fuego, agua, etc. (evitar)

Gestor de tareas de Windows: tenga cuidado al finalizar los procesos

Cuando trabaje en el Gestor de tareas de Windows, tenga cuidado de no finalizar ningún proceso que afecte al sistema de vigilancia. Si finaliza 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 sus datos antes de finalizar. Esto puede conducir a bases de datos de cámaras corruptas.

El Gestor de tareas de Windows suele mostrar una advertencia si se intenta finalizar un proceso. A menos que tenga la certeza absoluta de que la finalización del proceso no va a afectar al sistema de vigilancia, haga clic en **No** cuando el mensaje de advertencia le pregunte si realmente desea terminar el proceso.

Cortes de energía: usar un SAI

El motivo más común de las bases de datos corruptas es el cierre brusco del servidor de grabación, sin que se guarden los archivos y sin que el sistema operativo se cierre correctamente. Esto puede suceder debido a los cortes de energía, debido a que alguien accidentalmente tire del cable de alimentación del servidor, o algo parecido.

La mejor manera de proteger sus servidores de grabación para que no se apaguen bruscamente es equipar cada uno de sus servidores de grabación con un SAI (sistema de alimentación ininterrumpida).

El SAI funciona como una fuente de alimentación secundaria alimentada por batería, proporcionando la energía necesaria para guardar los archivos abiertos y apagar el sistema de forma segura en caso de irregularidades en la alimentación. Los SAI varían en sofisticación, pero muchos incluyen software para guardar automáticamente los archivos abiertos, para alertar a los administradores del sistema, etc.

La selección del tipo correcto de SAI para el entorno de su organización es un proceso individual. No obstante, cuando evalúe sus necesidades, tenga en cuenta la cantidad de tiempo de funcionamiento que necesita que el SAI sea capaz de proporcionar en caso de que falle la energía. Guardar los archivos abiertos y apagar un sistema operativo correctamente puede requerir varios minutos.

Registro de transacciones de la base de datos SQL (explicación)

Cada vez que se escribe un cambio en una base de datos SQL, la base de datos SQL registra este cambio en su registro de transacciones.

Con el registro de transacciones, se pueden revertir y deshacer los cambios en la base de datos SQL a través de Microsoft® SQL Server Management Studio. Por defecto, la base de datos SQL almacena su registro de transacciones indefinidamente, lo que con el tiempo significa que el registro de transacciones tiene cada vez más entradas. El registro de transacciones se encuentra por defecto en la unidad del sistema, y si el registro de transacciones sigue creciendo, puede impedir que Windows funcione correctamente.

Para evitar este tipo de situaciones, es conveniente vaciar el registro de transacciones con regularidad. La purga no hace que el archivo de registro de transacciones sea más pequeño, sino que limpia su contenido y evita así que crezca de forma descontrolada. Su sistema VMS no purga los registros de transacciones. En SQL Server, hay formas de vaciar el registro de transacciones. Visite la página de soporte de Microsoft https://docs.microsoft.com/en-us/sql/relational-databases/logs/the-transaction-log-sql-server?view=sql-server-2017 y busque *Truncamiento del registro de transacciones*.

Requisitos mínimos del sistema

Para obtener información acerca de los requisitos de sistema para las distintas aplicaciones del VMS y componentes del sistema, vaya al sitio web de Milestone (https://www.milestonesys.com/systemrequirements/).

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 de sistema para las distintas aplicaciones del VMS y componentes del sistema, vaya al sitio web de Milestone (https://www.milestonesys.com/systemrequirements/).

Microsoft® .NET Framework

Compruebe que todos los servidores poseen Microsoft .NET Framework 4.8 o superior instalado.

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.

Preparar Active Directory

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

Para facilitar la gestión de usuarios y grupos, Milestone recomienda tener instalado y configurado Microsoft Active Directory® antes de instalar el sistema XProtect. Si añade el servidor de gestión al Active Directory después de instalar el sistema, deberá reinstalar el servidor de gestión y sustituir los usuarios por los nuevos usuarios de Windows definidos en el Active Directory.

Los usuarios básicos no están soportados en los sistemas Milestone Federated Architecture, por lo que si planea utilizar Milestone Federated Architecture, debe añadir usuarios como usuarios de Windows a través del servicio de Active Directory. Si no instala Active Directory, siga los pasos en Instalación para grupos de trabajo en la página 183 cuando realice la instalación.

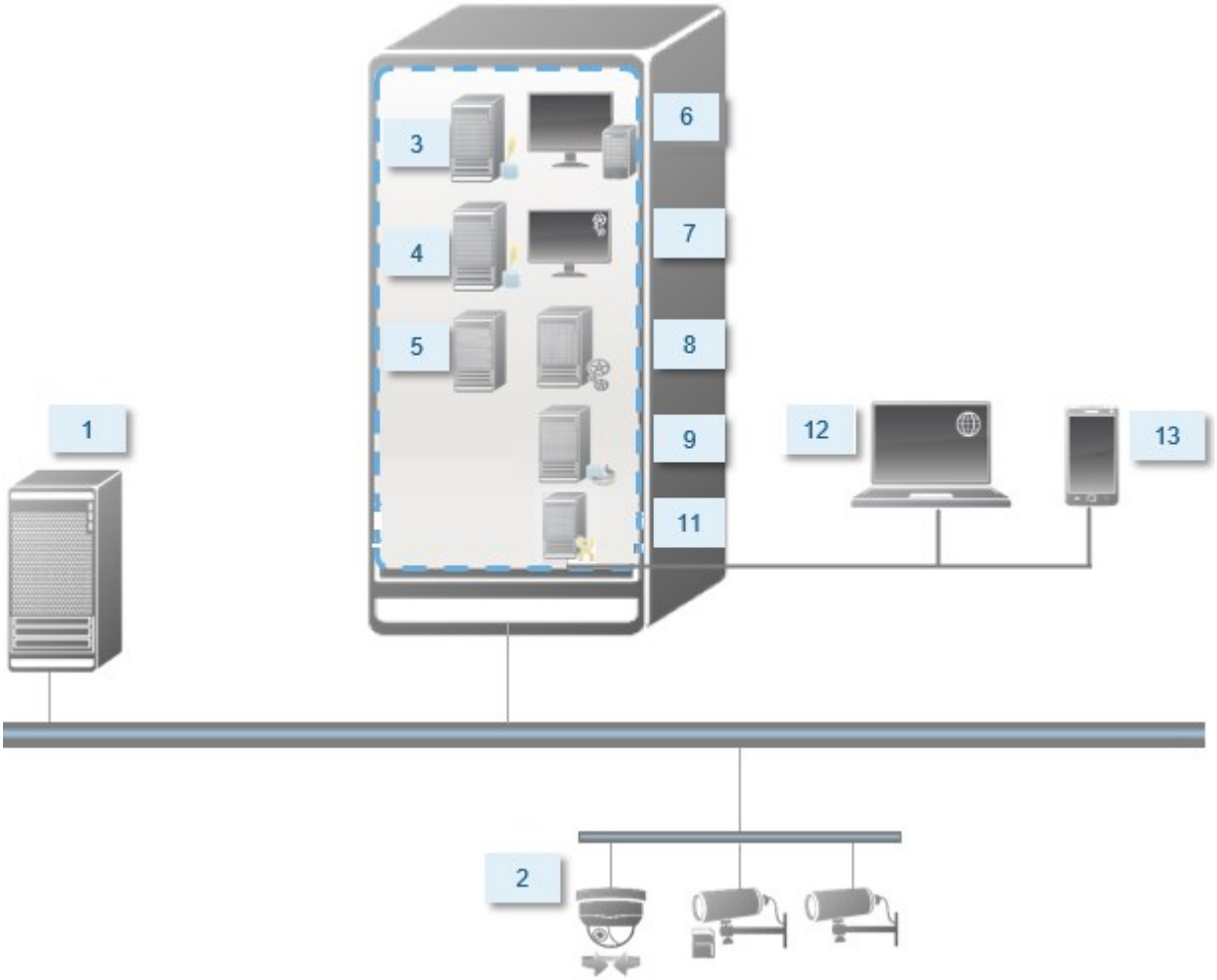
Método de instalación

Como parte del asistente de instalación, debe decidir qué método de instalación utilizar. Debe basar su selección en las necesidades de su organización, pero es muy probable que ya haya decidido el método cuando adquirió el sistema.

Opciones	Descripción
Único equipo	Instala todos los componentes del servidor y del cliente, así como el SQL Server en el ordenador actual.

Opciones	Descripción
	Una vez finalizada la instalación, tendrá la posibilidad de configurar su sistema a través de un asistente. Si acepta continuar, el servidor de grabación escanea su red en busca de hardware y puede seleccionar los dispositivos de hardware que desea añadir a su sistema. El número máximo de dispositivos de hardware que se pueden añadir en el asistente de configuración depende de su licencia básica. Además, las cámaras están preconfiguradas en las vistas y se ha creado un cometido de operador por defecto. Después de la instalación, XProtect Smart Client se abre, y ya está en condiciones de utilizar el sistema.
Personalizada	El servidor de gestión siempre está seleccionado en la lista de componentes del sistema y siempre se instala, pero puede seleccionar libremente qué instalar en el equipo actual entre los demás componentes del servidor y del cliente. Por defecto, el servidor de grabación no está seleccionado en la lista de componentes, pero puede cambiarlo. Posteriormente podrá instalar los componentes no seleccionados en otros ordenadores.

Instalación en un solo equipo

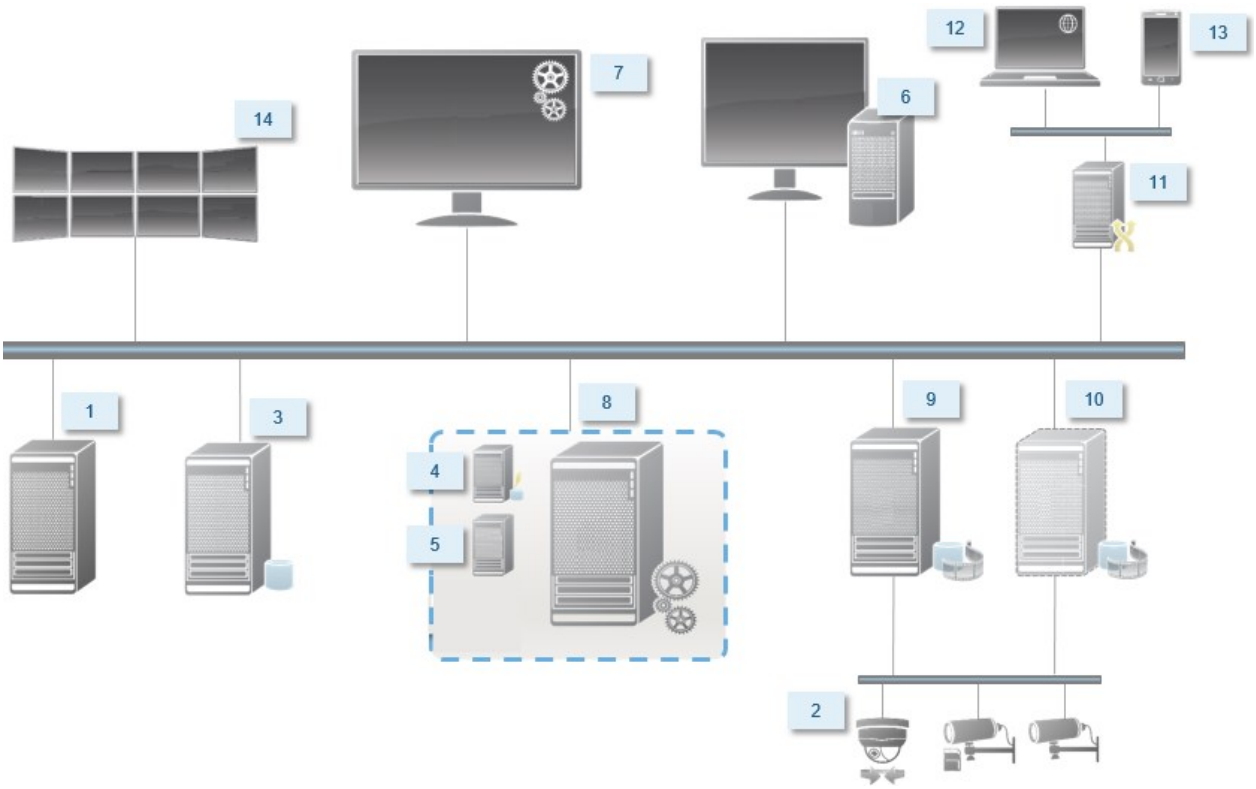


Componentes típicos de un sistema:

1. **Active Directory**
2. **Dispositivos**
3. **Servidor con SQL Server**
4. **Servidor de evento**
5. **Servidor de registro**
6. **XProtect Smart Client**
7. **Management Client**
8. **Servidor de gestión**
9. **Servidor de grabación**

10. **Servidor de grabación failover**
11. **XProtect Mobile servidor**
12. **XProtect Web Client**
13. **XProtect Mobile cliente**
14. **XProtect Smart Client con XProtect Smart Wall**

Instalación personalizada: ejemplo de componentes del sistema distribuido



Decidir sobre una edición de SQL Server

Microsoft® SQL Server® Express es una edición gratuita de SQL Server y es fácil de instalar y preparar para su uso en comparación con las otras ediciones de SQL Server. Durante una instalación de un **Único equipo**, se instala Microsoft SQL Server Express a menos que un SQL Server ya esté instalado en el equipo.

La instalación de XProtect VMS incluye la versión 2019 de Microsoft SQL Server Express. No todos los sistemas operativos de Windows son compatibles con esta edición de SQL Server. Antes de instalar XProtect VMS, compruebe que su sistema operativo es compatible con SQL Server 2019. Si su sistema operativo no es compatible con esta edición de SQL Server, instale una edición compatible de SQL Server antes de iniciar la instalación de XProtect VMS. Para obtener información sobre las ediciones compatibles de SQL Server, consulte https://www.milestonesys.com/systemrequirements/.

Para sistemas muy grandes o con muchas transacciones hacia y desde las bases de datos SQL, Milestone recomienda utilizar una edición del Microsoft® SQL Server® Standard o Microsoft® SQL Server® Enterprise de SQL Server en un ordenador dedicado en la red y en un disco duro dedicado que no se utilice para otros fines. La instalación del SQL Server en su propia unidad mejora el rendimiento de todo el sistema.

Seleccione cuenta de servicio

Como parte de la instalación, se le pide que especifique una cuenta para ejecutar los servicios de Milestone en este ordenador. Los servicios siempre se ejecutan en esta cuenta, independientemente del usuario que haya iniciado sesión. Asegúrese de que la cuenta tiene todos los permisos de usuario necesarios, por ejemplo, los permisos adecuados para realizar tareas, el acceso adecuado a la red y a los archivos, y el acceso a las carpetas compartidas de la red.

Puede seleccionar una cuenta predefinida o una cuenta de usuario. Base su decisión en el entorno en el que desea instalar su sistema:

Entorno del dominio

En un entorno de dominio:

- Milestone recomienda que utilice la cuenta de servicio de red integrada

  Es más fácil de usar incluso si necesita ampliar el sistema a varios equipos.
- También puede utilizar 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 utilizar una cuenta de usuario local que tenga todos los permisos necesarios. A menudo esta es la cuenta de administrador.

> ⚠ Si ha instalado los componentes de su sistema en varios ordenadores, la cuenta de usuario seleccionada debe estar configurada en todos los ordenadores de sus instalaciones con idéntico nombre de usuario, contraseña y permisos de acceso.

Autenticación Kerberos (explicación)

Kerberos es un protocolo de autenticación de red basado en tickets. Está diseñado para proporcionar una autenticación fuerte para aplicaciones cliente/servidor o servidor/servidor.

Use la autentificación Kerberos como alternativa al antiguo protocolo de autentificación Microsoft NT LAN (NTLM).

La autenticación Kerberos requiere una autenticación mutua, en la que el cliente se autentifica ante el servicio y el servicio se autentifica ante el cliente. De esta manera se puede autentificar de forma más segura desde clientes de XProtect a los servidores de XProtect sin exponer la contraseña.

Para hacer posible la autenticación mutua en su XProtect VMS debe registrar Service Principal Names (SPN) en el directorio activo. Un SPN es un alias que identifica de forma única a una entidad como un servicio de servidor XProtect. Cada servicio que utilice la autenticación mutua debe tener un SPN registrado para que los clientes puedan identificar el servicio en la red. Sin un SPN correctamente registrado, la autentificación mutua no es posible.

La siguiente tabla enumera los diferentes servicios de Milestone con sus correspondientes números de puerto que debe registrar:

Servicio	Número de puerto
Management Server - IIS	80 - Configurable
Management Server - Interno	8080
Recording Server - Data Collector	7609
Failover Server	8990
Event Server	22331
LPR Server	22334

El número de servicios que debe registrar en el directorio activo depende de su instalación actual. Data Collector se instala automáticamente cuando se instala el Management Server, Recording Server, Event Server o servicio Failover Server.

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

Si ejecuta el servicio bajo una cuenta de servicio de usuario de red, debe registrar los dos SPN para cada equipo que ejecute este servicio.

Este es el esquema de denominación SPN de Milestone:

```
VideoOS/[Nombre de host DNS]:[Puerto]
VideoOS/[Nombre de dominio completo]:[Puerto]
```

El siguiente es un ejemplo de SPN para el servicio Recording Server que se ejecuta en un ordenador con los siguientes detalles:

```
Nombre de host: Servidor de grabación1
Dominio: Surveillance.com
```

SPN para registrar:

```
VideoOS/Servidor de grabación 1:7609
VideoOS/Servidor de grabación1.Surveillance.com:7609
```

Exclusiones del escaneo de virus (explicación)

Como en el caso de cualquier otro software de base de datos, si se instala un programa antivirus en un ordenador que ejecuta el software XProtect, es importante que excluya determinados tipos de archivos y carpetas, así como cierto tráfico de red. Sin incluir estas excepciones, el escaneo antivirus usa una cantidad considerable de recursos del sistema. Además de eso, el proceso de escaneado puede bloquear temporalmente archivos que pueden provocar interrupciones o incluso daños en las bases de datos.

Cuando tenga que realizar un análisis de virus, no analice 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 escaneos antivirus en directorios de almacenamiento de archivos.

Cree las siguientes excepciones adicionales:

- Tipos de archivos: .blk, .idx, .pic
- Carpetas y subcarpetas:
  - `C:\Program Files\Milestone` o `C:\Program Files (x86)\Milestone`
  - `C:\ProgramData\Milestone\IDP\Registros`
  - `C:\ProgramData\Milestone`\KeyManagement\Registros
  - `C:\ProgramData\Milestone\MIPSDK`
  - `C:\ProgramData\Milestone\XProtect Data Collector Server\Registros`
  - `C:\ProgramData\Milestone\XProtect Servidor de evento\Registros`
  - `C:\ProgramData\Milestone\XProtect Servidor de registro`
  - `C:\ProgramData\Milestone\XProtect Servidor de gestión\Registros`
  - `C:\ProgramData\Milestone\XProtect Mobile Servidor\Registros`
  - `C:\ProgramData\Milestone\XProtect Servidor de grabación\Registros`
  - `C:\ProgramData\Milestone\XProtect Servidor web de informes\Registros`
  - `C:\ProgramData\Milestone\XProtect Recording Server\Secure\TablesDb`
- Excluir la exploración de la red en los siguientes puertos TCP:

Producto	puertos TCP
XProtect VMS	80, 8080, 7563, 25, 21, 9000
XProtect Mobile	8081

o

- Excluir la exploración de la red de los siguientes procesos:

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

Su organización puede tener directrices rigurosas en lo relativo a la detección de virus, pero es importante que las carpetas y los archivos mencionados se excluyan de la detección de virus.

¿Cómo se puede configurar XProtect VMS para que funcione en modo compatible con FIPS 140-2?

Para ejecutar XProtect VMS en un modo de operación FIPS 140-2 debe:

- Ejecute el sistema operativo Windows en el modo de funcionamiento aprobado por FIPS 140-2. Consulte el sitio de Microsoft para obtener información sobre la habilitación de FIPS.
- Garantizar que las integraciones independientes de terceros puedan ejecutarse en un sistema operativo Windows habilitado para FIPS
- Conectarse a los dispositivos de forma que se garantice un modo de funcionamiento conforme a FIPS 140-2
- Garantizar que los datos de la base de datos de los medios de comunicación están cifrados con cifrados que cumplan la norma FIPS 140-2

  Esto se hace ejecutando la herramienta de actualización de la base de datos de medios. Para obtener información detallada sobre cómo configurar su XProtect VMS para que se ejecute en modo compatible con FIPS 140-2, consulte la sección de cumplimiento de FIPS 140-2 la guía de endurecimiento.

Antes de instalar XProtect VMS en un sistema habilitado para FIPS

Aunque se pueden realizar nuevas instalaciones de XProtect VMS en ordenadores habilitados para FIPS, no puede actualizar XProtect VMS cuando FIPS está habilitado en el sistema operativo Windows.

Si está actualizando, antes de instalar, desactive la política de seguridad FIPS de Windows en todos los equipos que forman parte del VMS, incluido el equipo que aloja el servidor SQL.

El instalador XProtect VMS comprueba la política de seguridad FIPS y evitará que la instalación se inicie si FIPS está habilitado.

Pero, si está actualizando desde XProtect VMS versión 2020 R3 y posteriores, no necesita desactivar FIPS.

Una vez instalados los componentes XProtect VMS en todos los equipos y preparado el sistema para FIPS, puede habilitar la política de seguridad FIPS en Windows en todos los equipos de su VMS.

Para obtener información detallada sobre cómo configurar su XProtect VMS para que se ejecute en modo compatible con FIPS 140-2, consulte la sección de cumplimiento de FIPS 140-2 la guía de endurecimiento.

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.

Es posible instalar una versión gratuita de XProtect Essential+. Que le proporciona capacidades restringidas de XProtect VMS para un número limitado de cámaras. Deberá disponer de conexión a Internet para instalar XProtect Essential+.

El código de licencia del software (SLC) está impreso en la confirmación del pedido y el archivo de licencia del software lleva el nombre de su SLC.

Milestone recomienda que registre su SLC en nuestro sitio web (https://online.milestonesys.com/) antes de la instalación. Es posible que el distribuidor ya lo haya hecho.

Controladores de dispositivos (explicación)

Su sistema utiliza los controladores de dispositivos de vídeo para controlar y comunicarse con los dispositivos de cámara conectados a un servidor de grabación. Debe instalar los drivers de los dispositivos en cada servidor de grabación de su sistema.

A partir de la versión 2018 R1, los drivers de dispositivos se dividen en dos paquetes de dispositivos: el paquete de dispositivos normal con drivers más nuevos y un paquete de dispositivos heredados con controladores más antiguos.

El paquete de dispositivos normal se instala automáticamente al instalar el servidor de grabación. Posteriormente, puede actualizar los drivers descargando e instalando una versión más reciente del paquete de dispositivos. Milestone publica regularmente nuevas versiones de los drivers de los dispositivos y los pone a disposición en la página de descargas (https://www.milestonesys.com/downloads/) en nuestro sitio web como paquetes de dispositivos. Cuando actualiza un paquete de dispositivos, puede instalar la última versión sobre cualquier versión que tenga instalada.

El paquete de dispositivos heredados solo puede instalarse si el sistema tiene instalado un paquete de dispositivos normal. Los drivers del paquete de dispositivos heredados se instalan automáticamente si ya hay una versión anterior instalada en su sistema. Está disponible para su descarga e instalación manual en la página de descarga de software (https://www.milestonesys.com/downloads/).

Detenga el servicio de Recording Server antes de la instalación, de lo contrario tendrá que reiniciar el ordenador.

Para garantizar el mejor rendimiento, utilice siempre la última versión de los drivers de los dispositivos.

Requisitos para la instalación fuera de línea

Si instala el sistema en un servidor que está desconectado, necesita lo siguiente:

- El archivo `Milestone XProtect VMS Products 2023 R2 System Installer.exe`
- El archivo de licencia de software (SLC) para su sistema XProtect
- Medios de instalación del sistema operativo, incluida la versión de .NET necesaria (https://www.milestonesys.com/systemrequirements/)

Comunicación segura (explicación)

El Protocolo de Transferencia de Hipertexto Seguro (HTTPS) es una extensión del Protocolo de Transferencia de Hipertexto (HTTP) para la comunicación segura a través de una red informática. En HTTPS, el protocolo de comunicación está cifrado mediante Transport Layer Security (TLS), o su predecesor, Secure Sockets Layer (SSL).

En XProtect VMS, la comunicación segura se obtiene utilizando TLS/SSL con cifrado asimétrico (RSA).

TLS/SSL utiliza un par de claves, una privada y otra pública, para autenticar, asegurar y gestionar las conexiones seguras.

Una autoridad de certificación (CA) es cualquiera que pueda emitir certificados raíz. Puede tratarse de un servicio de Internet que emita certificados raíz, o de cualquier persona que genere y distribuya manualmente un certificado. Una CA puede emitir certificados para servicios web, es decir, para cualquier software que utilice la comunicación https. Este certificado contiene dos claves, una clave privada y una clave pública. La clave pública se instala en los clientes de un servicio web (clientes del servicio) mediante la instalación de un certificado público. La clave privada se utiliza para firmar los certificados del servidor que deben instalarse en el mismo. Siempre que un cliente de servicio llama al servicio web, el servicio web envía el certificado del servidor, incluida la clave pública, al cliente. El cliente de servicio puede validar el certificado del servidor utilizando el certificado de CA público ya instalado. El cliente y el servidor pueden ahora utilizar los certificados público y privado del servidor para intercambiar una clave secreta y establecer así una conexión segura TLS/SSL.

Para los certificados distribuidos manualmente, los certificados deben ser instalados antes de que el cliente pueda realizar dicha verificación.

Vea Seguridad de capa de transporte para tener más información sobre TLS.

> **!** Los certificados tienen una fecha de caducidad. XProtect VMS no le avisará cuando un certificado esté a punto de caducar. Si un certificado caduca:
> • Los clientes dejarán de confiar en el servidor de grabación con el certificado caducado y, por tanto, no podrán comunicarse con él
> • Los servidores de grabación dejarán de confiar en el servidor de gestión con el certificado caducado y, por tanto, no podrán comunicarse con él
> • Los dispositivos móviles dejarán de confiar en el servidor móvil con el certificado caducado y, por tanto, no podrán comunicarse con él
>
> Para renovar los certificados, siga los pasos de esta guía como lo hizo cuando creó los certificados.

Si desea más información, consulte la guía de certificados sobre cómo asegurar sus instalaciones XProtect VMS.

Instalación

Instalar un nuevo sistema XProtect

Instalar XProtect Essential+

Es posible instalar una versión gratuita de XProtect Essential+. Que le proporciona capacidades restringidas de XProtect VMS para un número limitado de cámaras. Deberá disponer de conexión a Internet para instalar XProtect Essential+.

Esta versión se instala en un solo ordenador, utilizando la opción de instalación en un **Equipo único**. La opción de **Único equipo** instala todos los componentes del servidor y del cliente en el ordenador actual.

Milestone recomienda que lea atentamente la siguiente sección antes de realizar la instalación: Antes de comenzar la instalación en la página 139.

Para las instalaciones FIPS, XProtect VMS no se puede actualizar cuando FIPS está habilitado en el sistema operativo Windows. Antes de la instalación, desactive la política de seguridad FIPS de Windows en todos los equipos que formen parte del VMS, incluido el equipo que aloja el servidor SQL. Pero, si está actualizando desde la versión 2020 R3 y posteriores de XProtect VMS, no necesita desactivar FIPS. Para obtener información detallada sobre cómo configurar su XProtect VMS para que se ejecute en modo compatible con FIPS 140-2, consulte la sección de cumplimiento de FIPS 140-2 la guía de endurecimiento.

Tras 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 los dispositivos de hardware que desea añadir a su sistema. Las cámaras están preconfiguradas en vistas, y tiene la opción de habilitar otros dispositivos como micrófonos y altavoces. También tiene la opción de añadir usuarios al sistema con un cometido de operador o de administrador. Después de la instalación, XProtect Smart Client se abre, y ya está en condiciones de utilizar el sistema.

En caso contrario, si cierra el asistente de instalación, XProtect Management Client se abre, donde puede realizar configuraciones manuales como añadir dispositivos de hardware y usuarios al sistema.

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

1. Descargue el software de Internet (https://www.milestonesys.com/downloads/) y ejecute el archivo de `Milestone XProtect VMS Products 2023 R2 System Installer.exe`.
2. Los archivos de instalación se desempaquetan. Dependiendo de los ajustes de seguridad, aparecen una o más advertencias de seguridad de Windows®. Acéptelo y el desempaquetado continúa.
3. Cuando se finalice, aparecerá el asistente de instalación **Milestone XProtect VMS**.
    1. Seleccione el **Idioma** a utilizar durante la instalación (este no es el idioma que su sistema utiliza una vez instalado, se selecciona más tarde). Haga clic en **Continuar**.
    2. Lea el *Milestone Acuerdo de licencia para usuario final*. Seleccione la casilla **Acepto los términos de este acuerdo de licencia** y haga clic en **Continuar**.
    3. En la página de **Ajustes de privacidad**, seleccione si desea compartir los datos de uso y haga clic en **Continuar**.

        > No debe habilitar la recopilación de datos si quiere que el sistema tenga una instalación que cumpla con el RGPD de la UE. Para obtener más información sobre la protección de datos y la recopilación de datos de uso, consulte la guía de privacidad del RGPD.

        > Siempre puede cambiar la configuración de privacidad más adelante. Consulte también Ajustes del sistema (cuadro de diálogo Opciones).

    4. Haga clic en el enlace **XProtect Essential+** para descargar un archivo de licencia gratuito.

        El archivo de licencia gratuito se descarga y aparece en el campo **Introducir o navegar a la ubicación 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 página **Asignar una contraseña de configuración del sistema**, introduzca una contraseña que proteja la configuración del sistema. Necesitará esta contraseña en caso de recuperación del sistema o al ampliarlo, por ejemplo, al añadir clusters.

   > Es importante que guarde esta contraseña y la mantenga a salvo. Si pierde esta contraseña, puede comprometer su capacidad para recuperar la configuración del sistema.

   Si no desea que la configuración del sistema esté protegida por una contraseña, seleccione **Elijo no usar una contraseña de configuración del sistema y entiendo que la configuración del sistema no estará cifrada**.

   Haga clic en **Continuar**.

6. En la página **Asignar una contraseña de protección de datos del servidor móvil**, introduzca una contraseña para cifrar sus investigaciones. Como administrador del sistema, tendrá que introducir esta contraseña para acceder a los datos del servidor móvil en caso de recuperación del sistema o cuando amplíe su sistema con servidores móviles adicionales.

   > Debe guardar esta contraseña y mantenerla a salvo. No hacerlo puede comprometer su habilidad para recuperar datos del servidor móvil.

   Si no desea que sus investigaciones estén protegidas por una contraseña, seleccione **Elijo no utilizar una contraseña de protección de datos del servidor móvil y entiendo que las investigaciones no estarán cifradas**.

   Haga clic en **Continuar**.

7. En la página **Especificar ajustes del servidor de grabación**, especifique los diferentes ajustes del servidor de grabación:
    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. Milestone recomienda guardar las grabaciones de vídeo en una ubicación distinta a aquella en la que se instala el software y no en la unidad del sistema. La ubicación predeterminada es la unidad con más espacio disponible.
    4. En el campo **Tiempo de retención para grabaciones de vídeo**, defina durante cuánto tiempo quiere guardar las grabaciones. Puede introducir entre 1 y 365 000 días, donde 7 días es el periodo de retención predeterminado.
    5. Haga clic en **Continuar**.

8. En la página **Seleccionar cifrado**, puede asegurar los flujos de comunicación:

   - Entre los servidores de grabación, los colectores de datos y el servidor de gestión

     Para habilitar el cifrado para los flujos de comunicación internos, en la sección **Certificado del servidor**, seleccione un certificado.

     > ⚠ Si se cifra la conexión del servidor de grabación al servidor de gestión, el sistema requiere que también se cifre la conexión del servidor de gestión al servidor de grabación.

   - Entre los servidores de grabación y los clientes

     Para habilitar el cifrado entre los servidores de grabación y los componentes cliente que recuperan flujos de datos del servidor de grabación, en la sección **Certificado de medios de transmisión**, seleccione un certificado.

   - Entre el servidor móvil y los clientes

     Para habilitar el cifrado entre los componentes del cliente que recuperan flujos de datos del servidor móvil, en la sección **Certificado de medios de transmisión móvil**, seleccione un certificado.

   - Entre el servidor de eventos y los componentes que se comunican con el servidor de eventos

     Para habilitar el cifrado entre el servidor de eventos y los componentes que se comunican con él, incluido el LPR Server, en la sección **Servidor de eventos y add-ons**, seleccione un certificado.

   Puede utilizar el mismo archivo de certificado para todos los componentes del sistema o utilizar diferentes archivos de certificado en función de los componentes del sistema.

   Para obtener más información sobre cómo preparar su sistema para una comunicación segura, consulte:

   - Comunicación segura (explicación) en la página 150
   - La guía Milestone sobre certificados

   También puede activar el cifrado después de la instalación desde el Server Configurator en el icono de la bandeja Management Server Manager en el área de notificación.

9. En la página **Seleccionar la ubicación del archivo y el idioma del producto**, haga lo siguiente:

    1. En el campo **Ubicación del archivo**, seleccione la ubicación donde desee instalar el software.

        Si algún producto Milestone XProtect VMS ya está instalado en el ordenador, este campo está deshabilitado. El campo muestra la ubicación donde se instalará el componente.

    2. En **Idioma del producto**, seleccione el idioma en que instalar el producto XProtect.
    3. Haga clic en **Instalar**.

    El software se instala. Si ya no está instalado en el ordenador, Microsoft® SQL Server® Express y Microsoft IIS se instalan automáticamente durante la instalación.

10. Se le puede indicar que reinicie el ordenador. Después de reiniciar su ordenador, dependiendo de los ajustes de seguridad, aparecen una o más advertencias de seguridad de Windows. Acéptelos y la instalación se completará.
11. Cuando la instalación se completa, una lista muestra los componentes que están instalados en el ordenador.

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

    Si hace clic en **Cerrar** en este momento, omitirá el asistente de configuración y se abre XProtect Management Client. Puede configurar el sistema, por ejemplo añadir hardware y usuarios al sistema, en Management Client.

12. En la página **Introducir nombres de usuario y contraseñas** para el hardware, introduzca los nombres de usuario y las contraseñas para el hardware que haya cambiado respecto a los valores predeterminados del fabricante.

    El instalador escanea la red en busca de este hardware, así como del hardware con credenciales por defecto del fabricante.

    Haga clic en **Continuar** y espere mientras el sistema escanea buscando hardware.

13. En la página **Seleccionar el hardware para añadir al sistema**, seleccione el hardware que desea añadir al sistema. Haga clic en **Continuar** y espere mientras el sistema añade el hardware.

14. En la página **Configurar los dispositivos**, puede dar nombres descriptivos al hardware haciendo clic en el icono de edición situado junto al nombre del hardware. Este nombre precederá a los dispositivos de hardware.

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

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

    Haga clic en **Continuar** y espere mientras el sistema configura el hardware.

15. En la página **Añadir usuarios**, puede añadir usuarios al sistema como usuarios de Windows o usuarios básicos. Los usuarios pueden tener el cometido de Administradores o el de Operadores.

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

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

16. Cuando la instalación y la configuración inicial estén completadas, aparecerá la página **La configuración se ha completado**, donde verá:
    - Una lista de dispositivos de hardware que se añaden al sistema
    - Una lista de los usuarios añadidos a su sistema
    - Direcciones para el cliente XProtect Web Client y XProtect Mobile, que puede compartir con sus usuarios

    Cuando haga clic en **Cerrar**, XProtect Smart Client se abre y está listo para usarse.

Instalar el sistema: opción de Equipo único

La opción **Ordenador único** instala todos los componentes de servidor y cliente en el ordenador actual.

> Milestone recomienda que lea atentamente la siguiente sección antes de realizar la instalación: Antes de comenzar la instalación en la página 139.

> Para las instalaciones FIPS, XProtect VMS no se puede actualizar cuando FIPS está habilitado en el sistema operativo Windows. Antes de la instalación, desactive la política de seguridad FIPS de Windows en todos los equipos que formen parte del VMS, incluido el equipo que aloja el servidor SQL. Pero, si está actualizando desde la versión 2020 R3 y posteriores de XProtect VMS, no necesita desactivar FIPS. Para obtener información detallada sobre cómo configurar su XProtect VMS para que se ejecute en modo compatible con FIPS 140-2, consulte la sección de cumplimiento de FIPS 140-2 la guía de endurecimiento.

Tras 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 los dispositivos de hardware que desea añadir a su sistema. Las cámaras están preconfiguradas en vistas, y tiene la opción de habilitar otros dispositivos como micrófonos y altavoces. También tiene la opción de añadir usuarios al sistema con un cometido de operador o de administrador. Después de la instalación, XProtect Smart Client se abre, y ya está en condiciones de utilizar el sistema.

En caso contrario, si cierra el asistente de instalación, XProtect Management Client se abre, donde puede realizar configuraciones manuales como añadir dispositivos de hardware y usuarios al sistema.

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

1. Descargue el software de Internet (https://www.milestonesys.com/downloads/) y ejecute el archivo de `Milestone XProtect VMS Products 2023 R2 System Installer.exe`.
2. Los archivos de instalación se desempaquetan. Dependiendo de los ajustes de seguridad, aparecen una o más advertencias de seguridad de Windows®. Acéptelo y el desempaquetado continúa.
3. Cuando se finalice, aparecerá el asistente de instalación **Milestone XProtect VMS**.
    1. Seleccione el **Idioma** a utilizar durante la instalación (este no es el idioma que su sistema utiliza una vez instalado, se selecciona más tarde). Haga clic en **Continuar**.
    2. Lea el *Milestone Acuerdo de licencia para usuario final*. Seleccione la casilla **Acepto los términos de este acuerdo de licencia** y haga clic en **Continuar**.
    3. En la página de **Ajustes de privacidad**, seleccione si desea compartir los datos de uso y haga clic en **Continuar**.

> No debe habilitar la recopilación de datos si quiere que el sistema tenga una instalación que cumpla con el RGPD de la UE. Para obtener más información sobre la protección de datos y la recopilación de datos de uso, consulte la guía de privacidad del RGPD.

> Siempre puede cambiar la configuración de privacidad más adelante. Consulte también Ajustes del sistema (cuadro de diálogo Opciones).

4. En **Introducir o navegar a la ubicación del archivo de licencia**, introduzca su archivo de licencia desde su proveedor de XProtect. Alternativamente, navegue hasta la ubicación del archivo o haga clic en **XProtect Essential+** el enlace para descargar un archivo de licencia gratuito. Para conocer las limitaciones del producto gratuito XProtect Essential+, consulte la Comparación de productos en la página 116. El sistema verifica su archivo de licencia antes de poder continuar. 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 página **Asignar una contraseña de configuración del sistema**, introduzca una contraseña que proteja la configuración del sistema. Necesitará esta contraseña en caso de recuperación del sistema o al ampliarlo, por ejemplo, al añadir clusters.

   > Es importante que guarde esta contraseña y la mantenga a salvo. Si pierde esta contraseña, puede comprometer su capacidad para recuperar la configuración del sistema.

   Si no desea que la configuración del sistema esté protegida por una contraseña, seleccione **Elijo no usar una contraseña de configuración del sistema y entiendo que la configuración del sistema no estará cifrada**.

   Haga clic en **Continuar**.

6. En la página **Asignar una contraseña de protección de datos del servidor móvil**, introduzca una contraseña para cifrar sus investigaciones. Como administrador del sistema, tendrá que introducir esta contraseña para acceder a los datos del servidor móvil en caso de recuperación del sistema o cuando amplíe su sistema con servidores móviles adicionales.

   > Debe guardar esta contraseña y mantenerla a salvo. No hacerlo puede comprometer su habilidad para recuperar datos del servidor móvil.

   Si no desea que sus investigaciones estén protegidas por una contraseña, seleccione **Elijo no utilizar una contraseña de protección de datos del servidor móvil y entiendo que las investigaciones no estarán cifradas**.

   Haga clic en **Continuar**.

7. En la página **Especificar ajustes del servidor de grabación**, especifique los diferentes ajustes del servidor de grabación:

   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. Milestone recomienda guardar las grabaciones de vídeo en una ubicación distinta a aquella en la que se instala el software y no en la unidad del sistema. La ubicación predeterminada es la unidad con más espacio disponible.
   4. En el campo **Tiempo de retención para grabaciones de vídeo**, defina durante cuánto tiempo quiere guardar las grabaciones. Puede introducir entre 1 y 365 000 días, donde 7 días es el periodo de retención predeterminado.
   5. Haga clic en **Continuar**.

8. En la página **Seleccionar cifrado**, puede asegurar los flujos de comunicación:

   - Entre los servidores de grabación, los colectores de datos y el servidor de gestión

     Para habilitar el cifrado para los flujos de comunicación internos, en la sección **Certificado del servidor**, seleccione un certificado.

     > ⚠ Si se cifra la conexión del servidor de grabación al servidor de gestión, el sistema requiere que también se cifre la conexión del servidor de gestión al servidor de grabación.

   - Entre los servidores de grabación y los clientes

     Para habilitar el cifrado entre los servidores de grabación y los componentes cliente que recuperan flujos de datos del servidor de grabación, en la sección **Certificado de medios de transmisión**, seleccione un certificado.

   - Entre el servidor móvil y los clientes

     Para habilitar el cifrado entre los componentes del cliente que recuperan flujos de datos del servidor móvil, en la sección **Certificado de medios de transmisión móvil**, seleccione un certificado.

   - Entre el servidor de eventos y los componentes que se comunican con el servidor de eventos

     Para habilitar el cifrado entre el servidor de eventos y los componentes que se comunican con él, incluido el LPR Server, en la sección **Servidor de eventos y add-ons**, seleccione un certificado.

   Puede utilizar el mismo archivo de certificado para todos los componentes del sistema o utilizar diferentes archivos de certificado en función de los componentes del sistema.

   Para obtener más información sobre cómo preparar su sistema para una comunicación segura, consulte:

   - Comunicación segura (explicación) en la página 150
   - La guía Milestone sobre certificados

   También puede activar el cifrado después de la instalación desde el Server Configurator en el icono de la bandeja Management Server Manager en el área de notificación.

9. En la página **Seleccionar la ubicación del archivo y el idioma del producto**, haga lo siguiente:

    1. En el campo **Ubicación del archivo**, seleccione la ubicación donde desee instalar el software.

        Si algún producto Milestone XProtect VMS ya está instalado en el ordenador, este campo está deshabilitado. El campo muestra la ubicación donde se instalará el componente.

    2. En **Idioma del producto**, seleccione el idioma en que instalar el producto XProtect.
    3. Haga clic en **Instalar**.

    El software se instala. Si ya no está instalado en el ordenador, Microsoft® SQL Server® Express y Microsoft IIS se instalan automáticamente durante la instalación.

10. Se le puede indicar que reinicie el ordenador. Después de reiniciar su ordenador, dependiendo de los ajustes de seguridad, aparecen una o más advertencias de seguridad de Windows. Acéptelos y la instalación se completará.
11. Cuando la instalación se completa, una lista muestra los componentes que están instalados en el ordenador.

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

    Si hace clic en **Cerrar** en este momento, omitirá el asistente de configuración y se abre XProtect Management Client. Puede configurar el sistema, por ejemplo añadir hardware y usuarios al sistema, en Management Client.

12. En la página **Introducir nombres de usuario y contraseñas** para el hardware, introduzca los nombres de usuario y las contraseñas para el hardware que haya cambiado respecto a los valores predeterminados del fabricante.

    El instalador escanea la red en busca de este hardware, así como del hardware con credenciales por defecto del fabricante.

    Haga clic en **Continuar** y espere mientras el sistema escanea buscando hardware.

13. En la página **Seleccionar el hardware para añadir al sistema**, seleccione el hardware que desea añadir al sistema. Haga clic en **Continuar** y espere mientras el sistema añade el hardware.

14. En la página **Configurar los dispositivos**, puede dar nombres descriptivos al hardware haciendo clic en el icono de edición situado junto al nombre del hardware. Este nombre precederá a los dispositivos de hardware.

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

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

    Haga clic en **Continuar** y espere mientras el sistema configura el hardware.

15. En la página **Añadir usuarios**, puede añadir usuarios al sistema como usuarios de Windows o usuarios básicos. Los usuarios pueden tener el cometido de Administradores o el de Operadores.

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

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

16. Cuando la instalación y la configuración inicial estén completadas, aparecerá la página **La configuración se ha completado**, donde verá:
    - Una lista de dispositivos de hardware que se añaden al sistema
    - Una lista de los usuarios añadidos a su sistema
    - Direcciones para el cliente XProtect Web Client y XProtect Mobile, que puede compartir con sus usuarios

    Cuando haga clic en **Cerrar**, XProtect Smart Client se abre y está listo para usarse.

Instale su sistema: opción personalizada

La opción **Personalizada** instala el servidor de gestión, pero puede seleccionar qué otros componentes del servidor y del cliente desea instalar en el ordenador actual. Por defecto, el servidor de grabación no está seleccionado en la lista de componentes. Dependiendo de sus selecciones, puede instalar después los componentes del sistema no seleccionados en otros ordenadores. Para obtener más información sobre cada componente del sistema y su cometido, consulte Descripción general del producto en la página 31. La instalación en otros ordenadores se realiza a través de la página web de descarga del servidor de gestión denominada Download Manager. Para obtener más información sobre la instalación a través del Download Manager, consulte Download Manager/página web de descarga en la página 188.

> Milestone recomienda que lea atentamente la siguiente sección antes de realizar la instalación: Antes de comenzar la instalación en la página 139.

Para las instalaciones FIPS, XProtect VMS no se puede actualizar cuando FIPS está habilitado en el sistema operativo Windows. Antes de la instalación, desactive la política de seguridad FIPS de Windows en todos los equipos que formen parte del VMS, incluido el equipo que aloja el servidor SQL. Pero, si está actualizando desde la versión 2020 R3 y posteriores de XProtect VMS, no necesita desactivar FIPS. Para obtener información detallada sobre cómo configurar su XProtect VMS para que se ejecute en modo compatible con FIPS 140-2, consulte la sección de cumplimiento de FIPS 140-2 la guía de endurecimiento.

1. Descargue el software de Internet (https://www.milestonesys.com/downloads/) y ejecute el archivo de `Milestone XProtect VMS Products 2023 R2 System Installer.exe`.
2. Los archivos de instalación se desempaquetan. Dependiendo de los ajustes de seguridad, aparecen una o más advertencias de seguridad de Windows®. Acéptelo y el desempaquetado continúa.
3. Cuando se finalice, aparecerá el asistente de instalación **Milestone XProtect VMS**.
    1. Seleccione el **Idioma** a utilizar durante la instalación (este no es el idioma que su sistema utiliza una vez instalado, se selecciona más tarde). Haga clic en **Continuar**.
    2. Lea el *Milestone Acuerdo de licencia para usuario final*. Seleccione la casilla **Acepto los términos de este acuerdo de licencia** y haga clic en **Continuar**.
    3. En la página de **Ajustes de privacidad**, seleccione si desea compartir los datos de uso y haga clic en **Continuar**.

        No debe habilitar la recopilación de datos si quiere que el sistema tenga una instalación que cumpla con el RGPD de la UE. Para obtener más información sobre la protección de datos y la recopilación de datos de uso, consulte la guía de privacidad del RGPD.

        Siempre puede cambiar la configuración de privacidad más adelante. Consulte también Ajustes del sistema (cuadro de diálogo Opciones).

    4. En **Introducir o navegar a la ubicación del archivo de licencia**, introduzca su archivo de licencia desde su proveedor de XProtect. Alternativamente, navegue hasta la ubicación del archivo o haga clic en **XProtect Essential+** el enlace para descargar un archivo de licencia gratuito. Para conocer las limitaciones del producto gratuito XProtect Essential+, consulte la Comparación de productos en la página 116. El sistema verifica su archivo de licencia antes de poder continuar. Haga clic en **Continuar**.

4. Seleccione **Personalizado**. Aparece una lista de los componentes a instalar. Aparte del servidor de gestión, todos los componentes de la lista son opcionales. El servidor de grabación y el servidor móvil no están seleccionados por defecto. Seleccione los componentes del sistema que desea instalar y haga clic en **Continuar**.

   En los pasos siguientes, se instalan todos los componentes del sistema. Para un sistema más distribuido, instale menos componentes del sistema en este ordenador y los restantes en otros. Si no puede reconocer un paso de instalación, es probable que sea porque no ha seleccionado instalar el componente del sistema al que pertenece esta página. En ese caso, continúe con el siguiente paso. Consulte también Instalación a través de Download Manager (explicación) en la página 170, Instalar un servidor de grabación a través de Download Manager en la página 171, y Instalación silenciosa a través de una consola de línea de comandos (explicación) en la página 177.

5. La página **Seleccionar un sitio web en el IIS para usar con su sistema XProtect** se muestra solo si tiene más de un sitio web IIS disponible en el ordenador. Debe seleccionar el sitio web que utilizará con su sistema XProtect. Seleccione un sitio web con enlace HTTPS. Haga clic en **Continuar**.

   Si Microsoft® IIS no está instalado en el ordenador, se instala.

6. En la página **Seleccionar Microsoft SQL Server**, seleccione el SQL Server que desea usar. Consulte también Opciones SQL Server durante instalación personalizada en la página 169. Haga clic en **Continuar**.

   Si no tiene un SQL Server en su ordenador local, puede instalar Microsoft SQL Server Express, pero en un sistema distribuido más grande, normalmente usaría un SQL Server dedicado en su red.

7. En la página **Seleccionar base de datos** (solo se muestra si ha seleccionado una existente SQL Server), seleccione o cree una base de datos SQL para almacenar la configuración de su sistema. Si elige una base de datos SQL existente, decida si desea **Mantener** o **Sobrescribir** los datos existentes. Si va a realizar una actualización, seleccione conservar los datos existentes para no perder la configuración del sistema. Consulte también Opciones SQL Server durante instalación personalizada en la página 169. Haga clic en **Continuar**.

8. En la página **Ajustes de bases de datos**, seleccione **Dejar que el instalador cree o vuelva a crear una base de datos** o bien **Utilizar una base de datos precreada**.

9. Para que sus bases de datos se creen o recreen automáticamente, seleccione **Dejar que el instalador cree o vuelva a crear una base de datos**, y haga clic en **Continuar**.

10. Para utilizar bases de datos que configuró para tal fin o bases de datos ya creadas, seleccione **Utilizar una base de datos precreada**. Aparecerá la página **Configuración avanzada de bases de datos**.

    En la página **Configuración avanzada de bases de datos**, introduzca el servidor y el nombre de la base de datos de los componentes de XProtect y haga clic en el icono de actualización para verificar la conexión.

    Haga clic en **Continuar**.

11. En la página **Asignar una contraseña de configuración del sistema**, introduzca una contraseña que proteja la configuración del sistema. Necesitará esta contraseña en caso de recuperación del sistema o al ampliarlo, por ejemplo, al añadir clusters.

    > Es importante que guarde esta contraseña y la mantenga a salvo. Si pierde esta contraseña, puede comprometer su capacidad para recuperar la configuración del sistema.

    Si no desea que la configuración del sistema esté protegida por una contraseña, seleccione **Elijo no usar una contraseña de configuración del sistema y entiendo que la configuración del sistema no estará cifrada**.

    Haga clic en **Continuar**.

12. En la página **Asignar una contraseña de protección de datos del servidor móvil**, introduzca una contraseña para cifrar sus investigaciones. Como administrador del sistema, tendrá que introducir esta contraseña para acceder a los datos del servidor móvil en caso de recuperación del sistema o cuando amplíe su sistema con servidores móviles adicionales.

    > Debe guardar esta contraseña y mantenerla a salvo. No hacerlo puede comprometer su habilidad para recuperar datos del servidor móvil.

    Si no desea que sus investigaciones estén protegidas por una contraseña, seleccione **Elijo no utilizar una contraseña de protección de datos del servidor móvil y entiendo que las investigaciones no estarán cifradas**.

    Haga clic en **Continuar**.

13. En **Seleccionar cuenta de servicio para el servidor de grabación**, seleccione **Esta cuenta predefinida** o **Esta cuenta** para seleccionar la cuenta de servicio para el servidor de grabación.

    Si es necesario, introduzca una contraseña.

    > El nombre de usuario de la cuenta debe ser una sola palabra. No debe tener un espacio.

    Haga clic en **Continuar**.

14. En la página **Especificar ajustes del servidor de grabación**, especifique los diferentes ajustes del servidor de grabación:

    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. Milestone recomienda guardar las grabaciones de vídeo en una ubicación distinta a aquella en la que se instala el software y no en la unidad del sistema. La ubicación predeterminada es la unidad con más espacio disponible.
    4. En el campo **Tiempo de retención para grabaciones de vídeo**, defina durante cuánto tiempo quiere guardar las grabaciones. Puede introducir entre 1 y 365 000 días, donde 7 días es el periodo de retención predeterminado.
    5. Haga clic en **Continuar**.

15. En la página **Seleccionar cifrado**, puede asegurar los flujos de comunicación:

    - Entre los servidores de grabación, los colectores de datos y el servidor de gestión

      Para habilitar el cifrado para los flujos de comunicación internos, en la sección **Certificado del servidor**, seleccione un certificado.

      > Si se cifra la conexión del servidor de grabación al servidor de gestión, el sistema requiere que también se cifre la conexión del servidor de gestión al servidor de grabación.

    - Entre los servidores de grabación y los clientes

      Para habilitar el cifrado entre los servidores de grabación y los componentes cliente que recuperan flujos de datos del servidor de grabación, en la sección **Certificado de medios de transmisión**, seleccione un certificado.

    - Entre el servidor móvil y los clientes

      Para habilitar el cifrado entre los componentes del cliente que recuperan flujos de datos del servidor móvil, en la sección **Certificado de medios de transmisión móvil**, seleccione un certificado.

    - Entre el servidor de eventos y los componentes que se comunican con el servidor de eventos

      Para habilitar el cifrado entre el servidor de eventos y los componentes que se comunican con él, incluido el LPR Server, en la sección **Servidor de eventos y add-ons**, seleccione un certificado.

    Puede utilizar el mismo archivo de certificado para todos los componentes del sistema o utilizar diferentes archivos de certificado en función de los componentes del sistema.

    Para obtener más información sobre cómo preparar su sistema para una comunicación segura, consulte:

    - Comunicación segura (explicación) en la página 150
    - La guía Milestone sobre certificados

    También puede activar el cifrado después de la instalación desde el Server Configurator en el icono de la bandeja Management Server Manager en el área de notificación.

16. En la página **Seleccionar la ubicación del archivo y el idioma del producto**, seleccione la **Ubicación del archivo** para los archivos del programa.

    > Si algún producto Milestone XProtect VMS ya está instalado en el ordenador, este campo está deshabilitado. El campo muestra la ubicación donde se instalará el componente.

17. En el campo **Idioma del producto**, seleccione el idioma en que instalar el producto XProtect. Haga clic en **Instalar**.

    El software se instala. Cuando la instalación finalice, verá una lista de los componentes del sistema instalados correctamente. Haga clic en **Cerrar**.

18. Se le puede indicar que reinicie el ordenador. Después de reiniciar su ordenador, dependiendo de los ajustes de seguridad, aparecen una o más advertencias de seguridad de Windows. Acéptelos y la instalación se completará.

19. Configure su sistema en Management Client. Consulte Lista de tareas de configuración inicial en la página 196.

20. Dependiendo de sus selecciones, instale el resto de los componentes del sistema en otros ordenadores a través de Download Manager. Consulte Instalación a través de Download Manager (explicación) en la página 170.

Opciones SQL Server durante instalación personalizada

Decida qué SQL Server y base de datos utilizar con las siguientes opciones.

SQL Server opciones:

- **Instalar Microsoft® SQL Server® Express en este ordenador**: Esta opción solo se muestra si no tiene instalado un SQL Server
- **Usar el SQL Server en este ordenador**: Esta opción solo se muestra si un SQL Server ya está instalado un en el ordenador
- **Seleccione una SQL Server en su red a través de la búsqueda**: Le permite buscar todos los SQL Server que se pueden descubrir en su subred de red
- **Seleccione una SQL Server en su red**: Le permite introducir la dirección (nombre de host o dirección IP) de un SQL Server que no pueda encontrar a través de la búsqueda

Opciones de base de datos SQL:

- **Crear nueva base de datos**: Principalmente para instalaciones nuevas
- **Usar base de datos existente**: Principalmente para actualizar las instalaciones existentes. Milestone recomienda que reutilice la base de datos SQL existente y mantenga los datos existentes en ella, para no perder la configuración del sistema. También puede optar por sobrescribir los datos en la base de datos SQL

Instalar nuevos componentes XProtect

Instalación a través de Download Manager (explicación)

Si desea instalar los componentes del sistema en otros ordenadores que no estén instalados en el servidor de gestión, deberá instalar estos componentes del sistema a través del sitio web Management Server de descargas de Download Manager.

1. Desde el ordenador en el que está instalado Management Server, diríjase a la página web de descarga de Management Server. En el menú **Inicio** de Windows, seleccione **Milestone** > **Página de instalación administrativa** y anote o copie la dirección de Internet para utilizarla posteriormente cuando instale los componentes del sistema en los demás ordenadores. La dirección es normalmente *http://[management server address]/installation/Admin/default-en-US.htm*.
2. Inicie sesión en cada uno de los otros ordenadores para instalar uno o más de los otros componentes del sistema:
   - Recording Server (Si desea más información, consulte Instalar un servidor de grabación a través de Download Manager en la página 171 o Instalar un servidor de grabación de forma silenciosa en la página 179)
   - Management Client (Si desea más información, consulte Instale un Management Client a través de Download Manager en la página 171)
   - Smart Client
   - Event Server

     > ⚠ Si va a instalar el Event Server en un entorno compatible con FIPS, debe desactivar el modo FIPS 140-2 de Windows antes de la instalación.

   - Log Server (Si desea más información, consulte Instalar un servidor de registros de forma silenciosa en la página 182)
   - Mobile Server (Para obtener más información, consulte el manual para el servidor de XProtect Mobile)
3. Abra un navegador de Internet, introduzca la dirección de la página web de descarga de Management Server en el campo de dirección, y descargue el instalador correspondiente.
4. Ejecutar el instalador.

Consulte Instale su sistema: opción personalizada en la página 163 si tiene dudas sobre las selecciones y ajustes en los diferentes pasos de la instalación.

Instale un Management Client a través de Download Manager

Si hay varios administradores del sistema XProtect o simplemente quiere gestionar el sistema XProtect desde varios ordenadores, puede instalar el Management Client siguiendo las siguientes instrucciones.

El Management Client se instala siempre en el servidor de gestión.

1. Desde el ordenador en el que está instalado Management Server, diríjase a la página web de descarga de Management Server. En el menú **Inicio** de Windows, seleccione **Milestone** > **Página de instalación administrativa** y anote o copie la dirección de Internet para utilizarla posteriormente cuando instale los componentes del sistema en los demás ordenadores. La dirección es normalmente *http://[management server address]/installation/Admin/default-en-US.htm*.
2. Inicie sesión en el ordenador donde desea instalar el componente del sistema.
1. Abra un navegador de Internet e introduzca la dirección de la página web de descarga de Management Server en el campo de dirección y pulse Enter.
3. Haga clic en **Todos los idiomas** para el instalador Management Client. Ejecute el archivo descargado.
4. Haga clic en **Sí** en todos los avisos. Comienza la descompresión.
5. Seleccione el idioma del instalador. Haga clic en **Continuar**.
6. Lea y acepte los términos del acuerdo de licencia. Haga clic en **Continuar**.
7. Seleccione la ubicación de los archivos y el idioma del producto. Haga clic en **Instalar**.
8. La instalación ha terminado. Se muestra una lista de todos los componentes instalados. Haga clic en **Cerrar**.
9. Haga clic en el icono que hay en el escritorio para abrir Management Client.
10. Aparece el diálogo de inicio de sesión de Management Client.
11. Especifique el nombre de host o la dirección IP de su servidor de gestión en el campo **Equipo**.
12. Seleccione autenticación, introduzca el nombre de usuario y la contraseña. Haga clic en **Conectar**. Se inicia Management Client.

    Para obtener más detalles sobre las funciones de Management Client y posibilidades de su sistema, haga clic en **Ayuda** en el menú de herramientas.

Instalar un servidor de grabación a través de Download Manager

Si los componentes de su sistema están distribuidos en ordenadores separados, puede instalar los servidores de grabación siguiendo las siguientes instrucciones.

El servidor de grabación ya está instalado si ha realizado una instalación con un **Equipo único**, pero puede utilizar las mismas instrucciones para añadir más servidores de grabación si necesita más capacidad.

Si necesita instalar un servidor de grabación de failover, consulte Instalar un servidor de grabación de failover a través de Download Manager en la página 175.

1. Desde el ordenador en el que está instalado Management Server, diríjase a la página web de descarga de Management Server. En el menú **Inicio** de Windows, seleccione **Milestone** > **Página de instalación administrativa** y anote o copie la dirección de Internet para utilizarla posteriormente cuando instale los componentes del sistema en los demás ordenadores. La dirección es normalmente *http://[management server address]/installation/Admin/default-en-US.htm*.
2. Inicie sesión en el ordenador donde desea instalar el componente del sistema.
3. Abra un navegador de Internet e introduzca la dirección de la página web de descarga de Management Server en el campo de dirección y pulse Enter.
4. Descargue el instalador del servidor de grabación seleccionando **Todos los idiomas** debajo del **Instalador del servidor de grabación**. Guarde el instalador o ejecútelo directamente desde la página web.
5. Seleccione el **Idioma** que desea utilizar durante la instalación. Haga clic en **Continuar**.
6. En la página **Seleccionar un tipo de instalación**, seleccione:

   Típico para instalar un servidor de grabación con valores por defecto, o

   Personalizado para instalar un servidor de grabación con valores personalizados.

7. En la página **Especificar ajustes del servidor de grabación**, especifique los diferentes ajustes del servidor de grabación:
    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. Milestone recomienda guardar las grabaciones de vídeo en una ubicación distinta a aquella en la que se instala el software y no en la unidad del sistema. La ubicación predeterminada es la unidad con más espacio disponible.
    4. En el campo **Tiempo de retención para grabaciones de vídeo**, defina durante cuánto tiempo quiere guardar las grabaciones. Puede introducir entre 1 y 365 000 días, donde 7 días es el periodo de retención predeterminado.
    5. Haga clic en **Continuar**.
8. La página **Direcciones IP de los servidores de grabación** solo se muestra si ha seleccionado **Personalizado**. Especifique el número de servidores de grabación que quiere instalar en este ordenador. Haga clic en **Continuar**.
9. En **Seleccionar cuenta de servicio para el servidor de grabación**, seleccione **Esta cuenta predefinida** o **Esta cuenta** para seleccionar la cuenta de servicio para el servidor de grabación.

    Si es necesario, introduzca una contraseña.

    > El nombre de usuario de la cuenta debe ser una sola palabra. No debe tener un espacio.

    Haga clic en **Continuar**.

10. En la página **Seleccionar cifrado**, puede asegurar los flujos de comunicación:

    - Entre los servidores de grabación, los colectores de datos y el servidor de gestión

      Para habilitar el cifrado para los flujos de comunicación internos, en la sección **Certificado del servidor**, seleccione un certificado.

      > Si se cifra la conexión del servidor de grabación al servidor de gestión, el sistema requiere que también se cifre la conexión del servidor de gestión al servidor de grabación.

    - Entre los servidores de grabación y los clientes

      Para habilitar el cifrado entre los servidores de grabación y los componentes cliente que recuperan flujos de datos del servidor de grabación, en la sección **Certificado de medios de transmisión**, seleccione un certificado.

    - Entre el servidor móvil y los clientes

      Para habilitar el cifrado entre los componentes del cliente que recuperan flujos de datos del servidor móvil, en la sección **Certificado de medios de transmisión móvil**, seleccione un certificado.

    - Entre el servidor de eventos y los componentes que se comunican con el servidor de eventos

      Para habilitar el cifrado entre el servidor de eventos y los componentes que se comunican con él, incluido el LPR Server, en la sección **Servidor de eventos y add-ons**, seleccione un certificado.

    Puede utilizar el mismo archivo de certificado para todos los componentes del sistema o utilizar diferentes archivos de certificado en función de los componentes del sistema.

    Para obtener más información sobre cómo preparar su sistema para una comunicación segura, consulte:

    - Comunicación segura (explicación) en la página 150
    - La guía Milestone sobre certificados

    También puede activar el cifrado después de la instalación desde el Server Configurator en el icono de la bandeja Management Server Manager en el área de notificación.

11. En la página **Seleccionar la ubicación del archivo y el idioma del producto**, seleccione la **Ubicación del archivo** para los archivos del programa.

    > Si algún producto Milestone XProtect VMS ya está instalado en el ordenador, este campo está deshabilitado. El campo muestra la ubicación donde se instalará el componente.

12. En el campo **Idioma del producto**, seleccione el idioma en que instalar el producto XProtect. Haga clic en **Instalar**.

    El software se instala. Cuando la instalación finalice, verá una lista de los componentes del sistema instalados correctamente. Haga clic en **Cerrar**.

13. Cuando haya instalado el servidor de grabación, puede comprobar su estado desde el icono de la bandeja Recording Server Manager y configurarlo en Management Client. Si desea más información, consulte Lista de tareas de configuración inicial en la página 196.

Instalar un servidor de grabación de failover a través de Download Manager

> ⚠ Si ejecuta grupos de trabajo, debe utilizar el método de instalación alternativo para los servidores de grabación de failover (consulte Instalación para grupos de trabajo en la página 183).

1. Desde el ordenador en el que está instalado Management Server, diríjase a la página web de descarga de Management Server. En el menú **Inicio** de Windows, seleccione **Milestone** > **Página de instalación administrativa** y anote o copie la dirección de Internet para utilizarla posteriormente cuando instale los componentes del sistema en los demás ordenadores. La dirección es normalmente *http://[management server address]/installation/Admin/default-en-US.htm*.

   Inicie sesión en el ordenador donde desea instalar el componente del sistema.

2. Abra un navegador de Internet e introduzca la dirección de la página web de descarga de Management Server en el campo de dirección y pulse Enter.

3. Descargue el instalador del servidor de grabación seleccionando **Todos los idiomas** debajo del **Instalador del servidor de grabación**. Guarde el instalador o ejecútelo directamente desde la página web.

4. Seleccione el **Idioma** que desea utilizar durante la instalación. Haga clic en **Continuar**.

5. En la página **Seleccionar un tipo de instalación**, seleccione **Failover** para instalar un servidor de grabación como servidor de grabación failover.

6. En la página **Especificar ajustes del servidor de grabación**, especifique los diferentes ajustes del servidor de grabación. El nombre del servidor de grabación de failover, la dirección del servidor de gestión y la ruta de acceso a la base de datos de medios. Haga clic en **Continuar**.

7. En la página **Seleccionar cuenta de servicio para el servidor de grabación** y al instalar un servidor de grabación de failover, debe utilizar la cuenta de usuario particular denominada **Esta cuenta**. Esto crea la cuenta de usuario failover. Si es necesario, introduzca una contraseña y confírmela. Haga clic en **Continuar**.

8. En la página **Seleccionar cifrado**, puede asegurar los flujos de comunicación:

   - Entre los servidores de grabación, los colectores de datos y el servidor de gestión

     Para habilitar el cifrado para los flujos de comunicación internos, en la sección **Certificado del servidor**, seleccione un certificado.

     > Si se cifra la conexión del servidor de grabación al servidor de gestión, el sistema requiere que también se cifre la conexión del servidor de gestión al servidor de grabación.

   - Entre los servidores de grabación y los clientes

     Para habilitar el cifrado entre los servidores de grabación y los componentes cliente que recuperan flujos de datos del servidor de grabación, en la sección **Certificado de medios de transmisión**, seleccione un certificado.

   - Entre el servidor móvil y los clientes

     Para habilitar el cifrado entre los componentes del cliente que recuperan flujos de datos del servidor móvil, en la sección **Certificado de medios de transmisión móvil**, seleccione un certificado.

   - Entre el servidor de eventos y los componentes que se comunican con el servidor de eventos

     Para habilitar el cifrado entre el servidor de eventos y los componentes que se comunican con él, incluido el LPR Server, en la sección **Servidor de eventos y add-ons**, seleccione un certificado.

   Puede utilizar el mismo archivo de certificado para todos los componentes del sistema o utilizar diferentes archivos de certificado en función de los componentes del sistema.

   Para obtener más información sobre cómo preparar su sistema para una comunicación segura, consulte:

   - Comunicación segura (explicación) en la página 150
   - La guía Milestone sobre certificados

   También puede activar el cifrado después de la instalación desde el Server Configurator en el icono de la bandeja Management Server Manager en el área de notificación.

9. En la página **Seleccionar la ubicación del archivo y el idioma del producto**, seleccione la **Ubicación del archivo** para los archivos del programa.

   > Si algún producto Milestone XProtect VMS ya está instalado en el ordenador, este campo está deshabilitado. El campo muestra la ubicación donde se instalará el componente.

10. En el campo **Idioma del producto**, seleccione el idioma en que instalar el producto XProtect. Haga clic en **Instalar**.

    El software se instala. Cuando la instalación finalice, verá una lista de los componentes del sistema instalados correctamente. Haga clic en **Cerrar**.

11. Cuando haya instalado el servidor de grabación failover, puede comprobar su estado desde el icono de la bandeja de servicio Failover Server y configurarlo en Management Client. Si desea más información, consulte Lista de tareas de configuración inicial en la página 196.

Instalación de XProtect VMS utilizando puertos no predeterminados

Una instalación de XProtect VMS requiere puertos concretos. En concreto, Management Server y API Gateway se ejecutan en el IIS, y determinados puertos deben estar disponibles. Este tema describe cómo instalar XProtect VMS y utilizar puertos no predeterminados en el IIS. Esto también es aplicable cuando solo se instala API Gateway.

Para ver una descripción general de todos los puertos que utiliza el VMS, consulte el manual del administrador de XProtect VMS (https://doc.milestonesys.com/2023r2/es-ES/portal/htm/chapter-page-mc-administrator-manual.htm).

Si IIS aún no está instalado en el sistema, el instalador de XProtect VMS instala IIS y utiliza el sitio web predeterminado con los puertos predeterminados.

Para evitar utilizar el XProtect VMS predeterminado, instale primero el IIS. Opcionalmente, añada un sitio web o proceda a utilizar el sitio web predeterminado.

Añada un enlace para HTTPS, si no existe ya, y seleccione un certificado válido en el ordenador (tendrá que seleccionarlo durante la instalación de XProtect VMS). Edite los números de puerto en los enlaces HTTP y HTTPS a los puertos disponibles que elija.

Ejecute el instalador de XProtect VMS y seleccione una instalación **Personalizada**.

Durante la instalación, aparece la página **Seleccione un sitio web en el IIS para usar con su sistema de XProtect** en el caso de que haya más de un sitio web disponible. Debe seleccionar el sitio web que utilizará con su sistema XProtect. El instalador utiliza los números de puerto cambiados.

Instalación silenciosa a través de una consola de línea de comandos (explicación)

Con la instalación silenciosa, los administradores de sistemas pueden instalar y actualizar el XProtect VMS y el software Smart Client a través de una gran red sin interacciones del usuario por su parte y con la menor molestia posible para los usuarios finales.

Los instaladores XProtect VMS y Smart Client (archivos .exe) tienen diferentes argumentos en la línea de comandos. Cada uno de ellos tiene su propio conjunto de parámetros de línea de comandos que pueden ser invocados directamente en una consola de línea de comandos o a través de un archivo de argumentos. En la consola de la línea de comandos, también puede utilizar las opciones de la línea de comandos con los instaladores.

Puede combinar los instaladores XProtect, sus parámetros de línea de comandos y sus opciones de línea de comandos con herramientas para la distribución e instalación silenciosa de software, como Microsoft System Center Configuration Manager (SCCM, también conocido como ConfigMgr). Para obtener más información sobre estas herramientas, visite el sitio web del fabricante. También puede utilizar Milestone Software Manager para la instalación y actualización remota de XProtect VMS, paquetes de dispositivos y Smart Client. Si desea más información, consulte el manual del administrador para Milestone Software Manager.

Parámetros de la línea de comandos y archivos de argumentos

Durante la instalación silenciosa, se pueden especificar ajustes que están relacionados directamente con los diferentes componentes del sistema VMS y su comunicación interna con parámetros de línea de comandos y archivos de argumentos. Los parámetros de la línea de comandos y los archivos de argumentos solo deben utilizarse para las nuevas instalaciones, ya que no se puede cambiar la configuración que representan los parámetros de la línea de comandos durante una actualización.

Para ver los parámetros disponibles en la línea de comandos y generar un archivo de argumentos para un instalador, en la consola de la línea de comandos, navegue hasta el directorio donde se encuentra el instalador e introduzca el siguiente comando:

```
[NameOfExeFile].exe --generateargsfile=[path]
```

Ejemplo:

```
MilestoneXProtectRecordingServerInstaller_x64.exe --generateargsfile=c:\temp
```

En el archivo de argumentos guardado (Arguments.xml), cada parámetro de la línea de comandos tiene una descripción que explica su propósito. Puede modificar y guardar el archivo de argumentos para que los valores de los parámetros de la línea de comandos se adapten a sus necesidades de instalación.

Si desea utilizar un archivo de argumentos con su instalador, utilice la opción de línea de comandos `--arguments` introduciendo el siguiente comando:

```
[NameOfExeFile].exe --quiet --arguments=[path]\[filename]
```

Ejemplo:

```
Milestone XProtect VMS Products 2023 R2 System Installer.exe --quiet
--arguments=C:\temp\arguments.xml
```

Opciones de línea de comandos

En la consola de línea de comandos, también puede combinar instaladores con opciones de línea de comandos. Las opciones de línea de comando generalmente modifican el comportamiento de un comando.

Para ver la lista completa de opciones de la línea de comandos, en la consola de la línea de comandos, navegue hasta el directorio donde se encuentra el instalador e introduzca `[NameOfExeFile].exe --help`. Para que la instalación tenga éxito, debe especificar un valor para las opciones de la línea de comandos que requieren un valor.

Puede utilizar tanto los parámetros como las opciones de la línea de comandos en el mismo comando. Use la opción de línea de comandos `--parameters` y divida cada parámetro de la línea de comandos con dos puntos (:). En el ejemplo siguiente, `--quiet`, `--showconsole`, y `--parameters` son opciones de línea de comandos, y `ISFAILOVER` y `RECORDERNAME` son parámetros de la línea de comandos:

```
MilestoneXProtectRecordingServerInstaller_x64.exe --quiet --showconsole
--parameters=ISFAILOVER:true:RECORDERNAME:Failover1
```

Instalar un servidor de grabación de forma silenciosa

Cuando lo instala de forma silenciosa, no se le notifica cuando la instalación se ha completado. Para recibir una notificación, incluya la opción de línea de comandos `--showconsole` en el comando. El icono de la bandeja Milestone XProtect Recording Server aparece cuando se completa la instalación.

En los ejemplos de comandos que aparecen a continuación, el texto dentro de los corchetes ([ ]) y los propios corchetes deben sustituirse por valores reales. Ejemplo: en lugar de "[ruta]" podría introducir **"d:\program files\"**, **d:\record**, o **\\network-storage-02\surveillance**. Utilice la opción de línea de comandos `--help` para leer sobre los formatos legales de cada valor de la opción de línea de comandos.

1. Inicie sesión en el ordenador donde desea instalar el componente Recording Server.
2. Abra un navegador de Internet e introduzca la dirección de la página web de descarga de Management Server que está dirigida a los administradores en el campo de dirección y pulse Intro.

   La dirección es normalmente `http://[management server address]:[port]/installation/Admin/default-en-US.htm`.
3. Descargue el instalador del servidor de grabación seleccionando **Todos los idiomas** debajo de **Instalador del servidor de grabación**.
4. Abra su consola de línea de comandos preferida. Para abrir el símbolo del sistema de Windows, abra el menú Inicio de Windows e introduzca **cmd**.
5. Navegue hasta el directorio con el instalador descargado.
6. Continúe la instalación en función de uno de los dos escenarios siguientes:

Escenario 1: Actualizar una instalación existente, o instalar en el servidor con el componente Management Server con valores por defecto

- Introduzca el siguiente comando y se iniciará la instalación.

```
MilestoneXProtectRecordingServerInstaller_x64.exe --quiet
```

Escenario 2: Instalar en un sistema distribuido

1. Introduzca el siguiente comando para generar un archivo de argumentos con los parámetros de la línea de comandos.

```
MilestoneXProtectRecordingServerInstaller_x64.exe --generateargsfile=
[path]
```

2. Abra el archivo de argumentos (Arguments.xml) desde la ruta especificada y modifique los valores de los parámetros de la línea de comandos si es necesario.

> Asegúrese de dar a los parámetros de la línea de comandos SERVERHOSTNAME y SERVERPORT valores válidos. Si no es así, la instalación no puede completarse.

4. Guarde el archivo de argumentos.
5. Vuelva a consola de línea de comandos e introduzca el siguiente comando para instalar con los valores de los parámetros de línea de comandos especificados en el archivo de argumentos.

```
MilestoneXProtectRecordingServerInstaller_x64.exe --quiet
--arguments=[path]\[filename]
```

Instalar XProtect Smart Client en silencio

Cuando lo instala de forma silenciosa, no se le notifica cuando la instalación se ha completado. Para recibir una notificación, incluya la opción de línea de comandos `--showconsole` en el comando. Una vez finalizada la instalación, aparecerá un acceso directo en el escritorio a XProtect Smart Client.

En los ejemplos de comandos que aparecen a continuación, el texto dentro de los corchetes ([ ]) y los propios corchetes deben sustituirse por valores reales. Ejemplo: en lugar de "[ruta]" podría introducir **"d:\program files\"**, **d:\record**, o **\\network-storage-02\surveillance**. Utilice la opción de línea de comandos `--help` para leer sobre los formatos legales de cada valor de la opción de línea de comandos.

1. Abra un navegador de Internet e introduzca la dirección de la página web de descarga de Management Server que está dirigida a los usuarios finales en el campo de dirección y pulse Enter.

   La dirección es normalmente `http://[management server address]:[port]/installation/default-en-US.htm`.

2. Descargue el instalador XProtect Smart Client seleccionando **Todos los idiomas** debajo de **Instalador de XProtect Smart Client**.
3. Abra su consola de línea de comandos preferida. Para abrir el símbolo del sistema de Windows, abra el menú Inicio de Windows e introduzca **cmd**.
4. Navegue hasta el directorio con el instalador descargado.
5. Continúe la instalación en función de uno de los dos escenarios siguientes:

   Escenario 1: Actualizar una instalación existente o instalar con los valores de los parámetros de la línea de comandos por defecto

   - Introduzca el siguiente comando y se iniciará la instalación.

     ```
     "XProtect Smart Client 2023 R2 Installer.exe" --quiet
     ```

   Escenario 2: Instalar con valores de parámetros de línea de comandos personalizados utilizando un archivo de argumentos xml como entrada

   1. Introduzca el siguiente comando para generar un archivo xml con los parámetros de la línea de comandos.

      ```
      "XProtect Smart Client 2023 R2 Installer.exe" --generateargsfile=[path]
      ```

   2. Abra el archivo de argumentos (Arguments.xml) desde la ruta especificada y modifique los valores de los parámetros de la línea de comandos si es necesario.
   3. Guarde el archivo de argumentos.
   4. Vuelva a consola de línea de comandos e introduzca el siguiente comando para instalar con los valores de los parámetros de línea de comandos especificados en el archivo de argumentos.

      ```
      "XProtect Smart Client 2023 R2 Installer.exe" --quiet --arguments=[path]\[filename]
      ```

Instalar un servidor de registros de forma silenciosa

Cuando lo instala de forma silenciosa, no se le notifica cuando la instalación se ha completado. Para recibir una notificación, incluya la opción de línea de comandos `--showconsole` en el comando.

En los ejemplos de comandos que aparecen a continuación, el texto dentro de los corchetes ([ ]) y los propios corchetes deben sustituirse por valores reales. Ejemplo: en lugar de "[ruta]" podría introducir **"d:\program files\"**, **d:\record**, o **\\network-storage-02\surveillance**. Utilice la opción de línea de comandos `--help` para leer sobre los formatos legales de cada valor de la opción de línea de comandos.

1. Inicie sesión en el ordenador donde desea instalar el componente Log Server.
2. Abra un navegador de Internet e introduzca la dirección de la página web de descarga de Management Server que está dirigida a los administradores en el campo de dirección y pulse Intro.

   La dirección es normalmente `http://[management server address]:[port]/installation/Admin/default-en-US.htm`.
3. Descargue el instalador del servidor de registros seleccionando **Todos los idiomas** debajo de **Instalador del servidor de registros**.
4. Abra su consola de línea de comandos preferida. Para abrir el símbolo del sistema de Windows, abra el menú Inicio de Windows e introduzca **cmd**.
5. Navegue hasta el directorio con el instalador descargado.
6. Continúe la instalación en función de uno de los dos escenarios siguientes:

   Escenario 1: Actualizar una instalación existente o instalar con los valores de los parámetros de la línea de comandos por defecto

   - Introduzca el siguiente comando y se iniciará la instalación.

     ```
     "XProtect Log Server 2023 R2 Installer x64.exe" --quiet --showconsole
     ```

   Escenario 2: Instalar con valores de parámetros de línea de comandos personalizados utilizando un archivo de argumentos xml como entrada

   1. Introduzca el siguiente comando para generar un archivo xml con los parámetros de la línea de comandos.

      ```
      "XProtect Log Server 2023 R2 Installer x64.exe" --generateargsfile=[path]
      ```
   2. Abra el archivo de argumentos (Arguments.xml) desde la ruta especificada y modifique los valores de los parámetros de la línea de comandos si es necesario.
   3. Guarde el archivo de argumentos.

4. Vuelva a consola de línea de comandos e introduzca el siguiente comando para instalar con los valores de los parámetros de línea de comandos especificados en el archivo de argumentos.

```
"XProtect Log Server 2023 R2 Installer x64.exe" --quiet --arguments=
[path]\[filename] --showconsole
```

Instalación para grupos de trabajo

Si no utiliza una configuración de dominio con un servidor de Active Directory, sino una configuración de grupo de trabajo, haga lo siguiente cuando lleve a cabo la instalación.

> Todos los ordenadores de una configuración distribuida deben estar en un dominio o en un grupo de trabajo.

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

   > Asegúrese de utilizar la misma cuenta en todos los ordenadores del sistema.

2. Dependiendo de sus necesidades, inicie la instalación del servidor de gestión o de grabación y haga clic en **Personalizado**.
3. Dependiendo de lo que haya seleccionado en el paso 2, seleccione instalar el Management Server o Recording Server el servicio utilizando una cuenta de administrador común.
4. Finalice la instalación.
5. Repita los pasos 1-4 para instalar cualquier otro sistema que desee conectar. Todos ellos deben ser instalados utilizando una cuenta de administrador común.

Instalar en un clúster

Antes de realizar la instalación en un clúster, consulte Múltiples servidores de gestión (clustering) (explicación) en la página 136 y Requisitos para el clustering en la página 137.

> Las descripciones e ilustraciones pueden diferir de lo que se ve en la pantalla.

Instalar el servidor de gestión:

1. Instale el servidor de gestión y todos sus subcomponentes en el primer servidor del clúster.

> El servidor de gestión debe instalarse con un usuario específico y no como un servicio de red. Para ello es necesario utilizar la opción de instalación **Personalizada**. Además, el usuario específico debe tener acceso a la unidad de red compartida y, preferiblemente, una contraseña que no caduque.

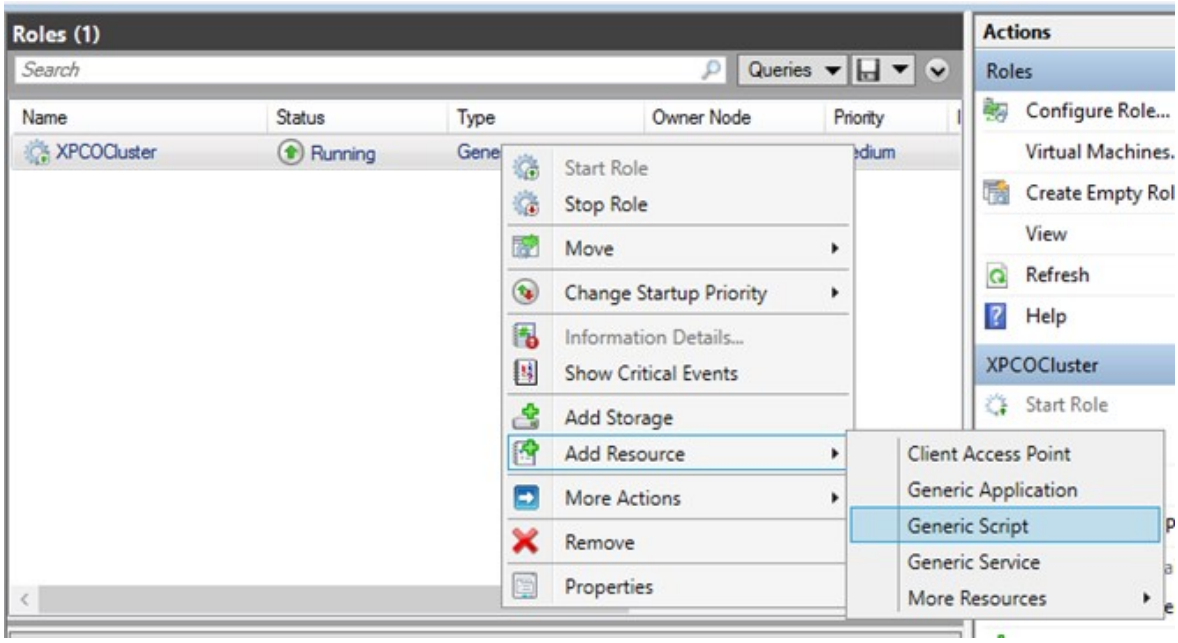
Configure el servicio Management Server como un servicio genérico en el cluster de failover:

1. En el último servidor en el que haya instalado el servidor de gestión, vaya a **Inicio** > **Herramientas administrativas**, abra la **Gestión de clústeres de failover** de Windows. En la ventana de **Administrador de clústeres de conmutación por error**, expanda su clúster, haga clic con el botón derecho en **Cometidos** y seleccione **Configurar un cometido**.

2. En la página **Asistente de alta disponibilidad** > página **Antes de comenzar**, haga clic en **Siguiente**.
3. En la página **Seleccionar cometido**, seleccione **Servicio genérico** y haga clic en **Siguiente**.
4. En la página **Seleccionar servicio**, seleccione el servicio **Milestone XProtect Management Server** y haga clic en **Siguiente**.
5. En la página **Punto de acceso del cliente** especifique el nombre (nombre de host del clúster) que los clientes utilizan cuando acceden al servicio. El nombre de host debe ser diferente del nombre del clúster. Haga clic en **Siguiente**.
6. En la página **Seleccionar almacenamiento**, haga clic en **Siguiente**, ya que no se requiere almacenamiento para el servicio.
7. En la página **Replicar configuración del registro**, haga clic en **Siguiente**, ya que no se debe replicar ningún ajuste del registro.
8. En la página **Confirmación**, haga clic en **Siguiente** después de haber verificado que el servicio de clúster está configurado de acuerdo con sus requisitos.
9. En la página **Configurar alta disponibilidad**, haga clic en **Siguiente**.

10. En la **página Resumen**, haga clic en **Finalizar** para completar la configuración del servidor de gestión como un servicio genérico en el clúster de conmutación por error.

11. Haga clic con el botón derecho en el cometido que acaba de crear y haga clic en **Agregar recurso** > **Secuencia de comandos genérica**. Seleccione Milestone XProtect Event Server para agregar el servicio **Milestone XProtect Event Server** como recurso al servicio **Milestone XProtect Management Server Cluster**.



12. Repita el paso 11 y añada todos los servicios necesarios en el clúster, por ejemplo, el Log Server. El Milestone XProtect Event Server y el Data Collector server deben añadirse como servicios para lograr una implementación óptima. Asimismo, el Milestone XProtect Event Server debe configurarse como un servicio dependiente del servidor de gestión, para asegurarse de que el servidor de eventos se detenga también cuando se detiene el servidor de gestión.

13. Todos los servicios añadidos se muestran en el panel inferior de la ventana.

Actualizar el clúster URL:

> Al realizar cambios en la configuración en el Gestor de clústeres de failover de Microsoft, pause el control y monitorice el servicio para que Server Configurator pueda hacer cambios e iniciar y/o parar el servicio de Management Server. Si cambia el tipo de inicio del servicio de clúster de failover, no debe provocar ningún conflicto con el Server Configurator.

En los ordenadores de Management Server:

1. Inicie Server Configurator en cada uno de los ordenadores que tienen un servidor de gestión instalado.
2. Vaya a la página **Registro**.
3. Haga clic en el símbolo del lápiz () para que la dirección del servidor de gestión sea editable.
4. Cambie la dirección del servidor de gestión a la URL del clúster, por ejemplo **http://MyCluster**.
5. Haga clic en **Registrar**.

En ordenadores que tienen componentes que utilizan el Management Server (por ejemplo, Recording Server, Mobile Server, Event Server, API Gateway):

1. Inicie Server Configurator en cada uno de los ordenadores.
2. Vaya a la página **Registro**.
3. Cambie la dirección del servidor de gestión a la URL del clúster, por ejemplo **http://MyCluster**.
4. Haga clic en **Registrar**.

Utilizar un certificado para un IDP externo en un entorno de clúster

Cuando instala XProtect en un entorno de un solo servidor, el IDP externo de datos de configuración se protege mediante la API de protección de datos (DPAPI). Si configura el servidor de gestión en un clúster, el IDP externo de datos de configuración debe estar protegido con un certificado para garantizar una conmutación por error de nodos fluida.

Para obtener más información sobre cómo generar un certificado, consulte La guía Milestone sobre certificados.

Debe importar el certificado al almacén de certificados personales y hacer que el certificado sea de confianza en el ordenador.

Para configurar la protección de datos debe añadir la huella del certificado a la configuración Identity Provider.

1. Importar el certificado al almacén de certificados personales y asegurarse de que:
   - el certificado es válido
   - la cuenta Identity Provider app pool (IDP) tiene permisos para la clave privada del certificado.

   Para más información sobre cómo verificar si la cuenta tiene permisos para la clave privada del certificado, consulte La guía Milestone sobre certificados.
2. Ubicar el archivo `appsettings.json` en la ruta de instalación del Identity Provider ("[Ruta de instalación]\Milestone\XProtect Management Server\IIS\Identity Provider").
3. Establecer la huella del certificado en la sección:

```
"DataProtectionSettings": {
"ProtectKeysWithCertificate": {
"Thumbprint": ""
}
},
```

4. Repetir el paso 3 en todos los nodos del servidor de gestión.
5. Aplique un failover de nodo para garantizar que la configuración del certificado es correcta.
6. Vuelva a iniciar sesión utilizando el cliente de gestión y aplique la configuración del proveedor externo. Si la configuración ya se ha aplicado, debe volver a introducir el secreto del cliente desde el IDP externo en el cliente de gestión.

Solución de errores cuando una configuración de IDP externo está protegida con un certificado

Certificado inválido/certificado caducado

Si el certificado de huella digital configurado representa un certificado que no es de confianza o ha caducado, el Identity Provider no puede iniciarse. El registro Identity Provider (`C:\ProgramData\Milestone\Identity Provider\Logs\Idp.log`) indicará claramente si el certificado no es válido.

Solución:

Asegúrese de que el certificado es válido y de confianza en el ordenador.

Falta de permisos para las claves privadas de los certificados

El Identity Provider no puede proteger los datos sin permisos para las claves privadas. Si el Identity Provider no tiene el permiso, se escribe el siguiente mensaje de error en el archivo de registro del Identity Provider (`C:\ProgramData\Milestone\Identity Provider\Logs\Idp.log`):

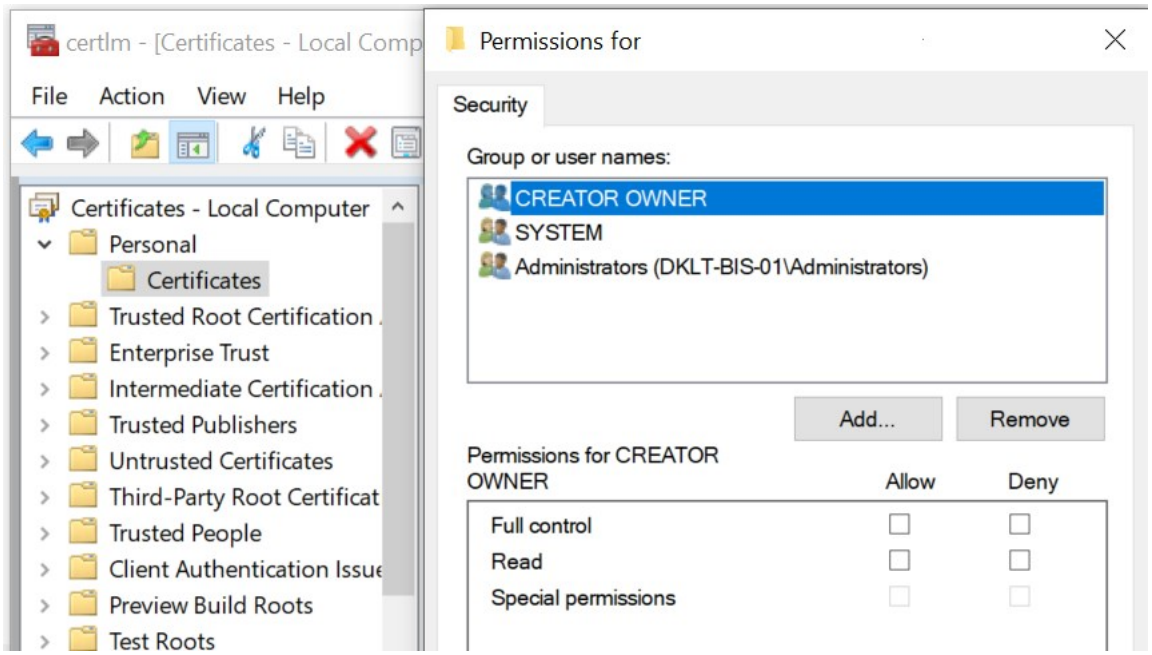
```
ERROR: se ha producido una excepción al procesar el elemento clave '<key
id="[específico de la instalación]" version="1" />'.
Internal.Cryptography.CryptoThrowHelper+WindowsCryptographicException: El
juego de llaves no existe
```

Solución:

Asegúrese de que la cuenta Identity Provider app pool (IDP) tiene permisos para las claves privadas del certificado.

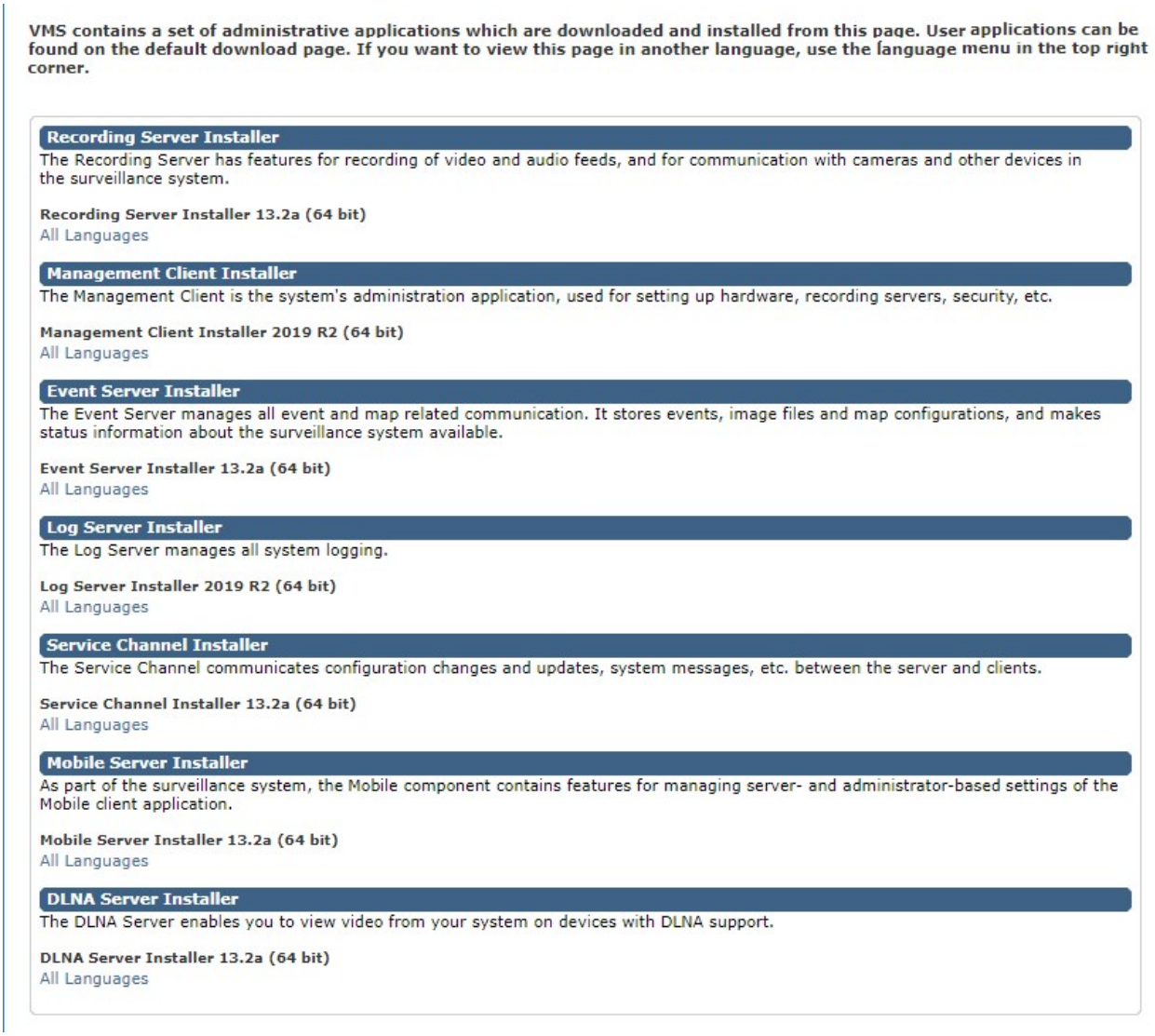
Compruebe los permisos de una clave privada de certificado:

1. Seleccione **Iniciar** en la barra de tareas de Windows y abra la herramienta Gestionar certificados del equipo (certlm.msc).
2. Navegue hasta el almacén de certificados personales y encuentre el certificado que se utiliza para el cifrado.
3. Haga clic con el botón derecho en el certificado y seleccione **Todas las tareas** > **Gestionar claves privadas**.
4. En **Permisos para**, asegúrese de que la cuenta de Identity Provider app pool (IDP) tiene permisos de lectura.



Download Manager/página web de descarga

El servidor de gestión tiene una página web integrada. Esta página web permite a los administradores y a los usuarios finales descargar e instalar los componentes necesarios del sistema XProtect desde cualquier lugar, de forma local o remota.



La página web puede mostrar dos conjuntos de contenidos, ambos en una versión de idioma que por defecto coincide con el idioma de la instalación del sistema:

- Una página web está dirigida a los **administradores**, permitiéndoles descargar e instalar componentes clave del sistema. La mayoría de las veces la página web se carga automáticamente al final de la instalación del servidor de gestión y se muestra el contenido por defecto. En el servidor de gestión, puede acceder a la página web desde el menú **Inicio** de Windows, seleccione **Programas** > **Milestone** > **Página de instalación administrativa**. De lo contrario, puede introducir la URL:

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

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

- Una página web está dirigida a los **usuarios** finales, proporcionándoles acceso a las aplicaciones cliente con la configuración por defecto. En el servidor de gestión, puede acceder a la página web desde el menú **Inicio** de Windows, seleccione **Programas** > **Milestone** > **Página de instalación pública**. De lo contrario, puede introducir la URL:

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

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

Las dos páginas web tienen un contenido predeterminado para que pueda utilizarlas inmediatamente después de la instalación. Sin embargo, como administrador, utilizando el Download Manager, puede personalizar lo que debe mostrarse en las páginas web. También puede mover componentes entre las dos versiones de la página web. Para mover un componente, haga clic con el botón derecho del ratón y seleccione la versión de la página web a la que desea mover el componente.

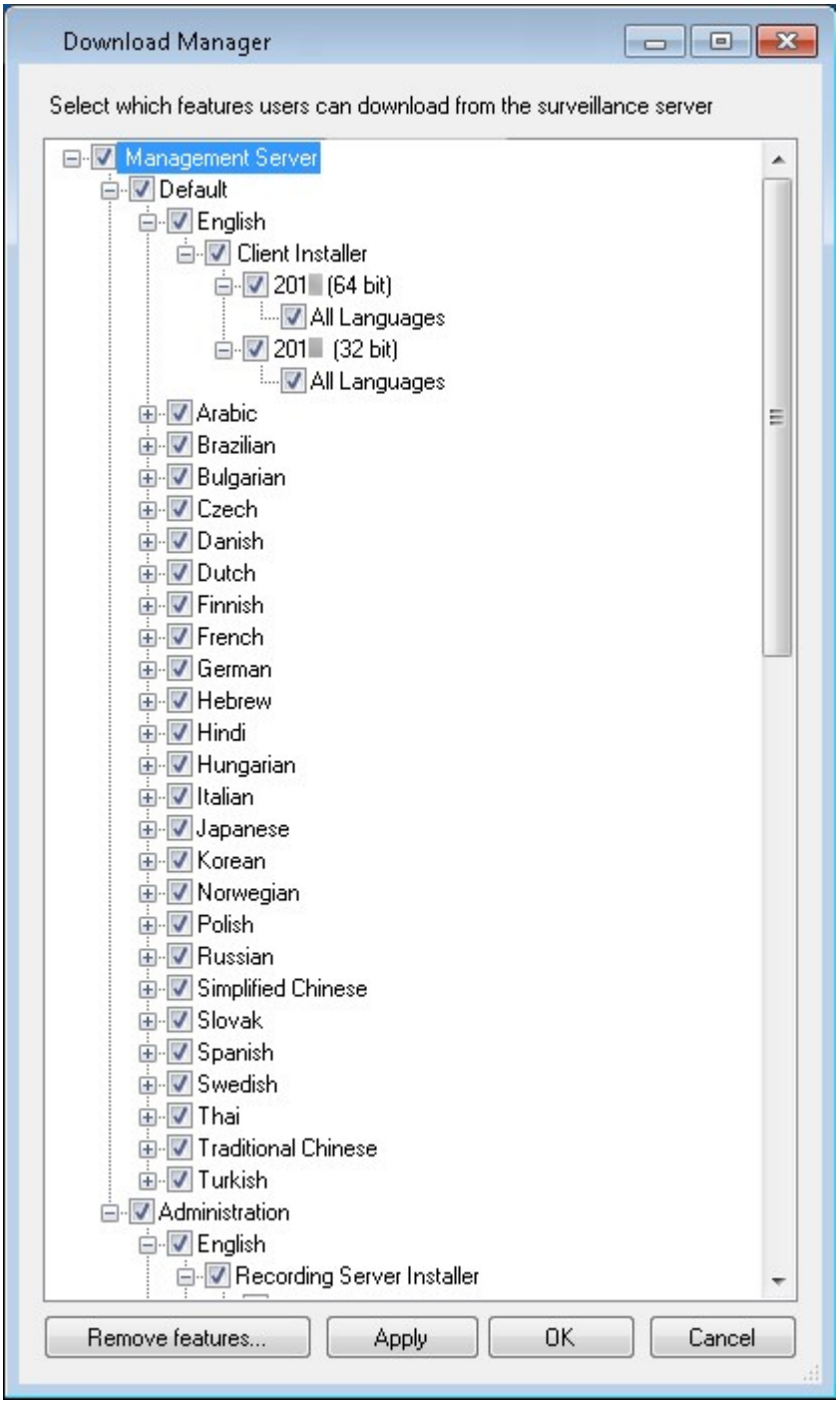
Aunque puede controlar qué componentes pueden descargar e instalar los usuarios en Download Manager, no puede utilizarla como herramienta de gestión de permisos de los usuarios. Estos permisos están determinados por los cometidos definidos en el Management Client.

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

Download Managerde la configuración por defecto

El Download Manager tiene una configuración por defecto. Esto garantiza que los usuarios de su organización puedan acceder a los componentes estándar desde el principio.

La configuración por defecto le proporciona una configuración por defecto con acceso a la descarga de componentes extra u opcionales. Normalmente se accede a la página web desde el ordenador del servidor de gestión, pero también se puede acceder a la página web desde otros equipos.



- El primer nivel: Hace referencia a su producto XProtect
- El segundo nivel: Hace referencia a las dos versiones de la página web a las que se dirige. **Por defecto** hace referencia a la versión de la página web que ven los usuarios finales. **Administración** hace referencia a la versión de la página web que ven los administradores del sistema
- El tercer nivel: Hace referencia a los idiomas en los que está disponible la página web

- El cuarto nivel: Hace referencia a los componentes que están, o pueden estar, a disposición de los usuarios
- El quinto nivel: Hace referencia a versiones concretas de cada componente, que están o pueden estar a disposición de los usuarios
- El sexto nivel: Hace referencia a las versiones lingüísticas de los componentes que están, o pueden estar, a disposición de los usuarios

El hecho de que solo estén disponibles inicialmente los componentes estándar y solo en la misma versión lingüística que el propio sistema, ayuda a reducir el tiempo de instalación y a ahorrar espacio en el servidor. No es necesario tener un componente o una versión del idioma disponible en el servidor si nadie lo utiliza.

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

Download Managerde los instaladores estándar (usuario)

Por defecto, los siguientes componentes están disponibles para su instalación por separado desde la página web de descargas del servidor de gestión dirigida a los usuarios (controlada por el Download Manager):

- Servidores de grabación, incluidos los de failover. Los servidores de grabación de failover se descargan e instalan inicialmente como servidores de grabación, durante el proceso de instalación se especifica que se desea un servidor de grabación de failover.
- Management Client
- XProtect Smart Client
- Servidor de eventos, utilizado en relación con la funcionalidad de los planos
- Servidor de registro, usado para proporcionar la funcionalidad necesaria para registrar la información del sistema
- Servidor XProtect Mobile
- Puede haber más opciones en su organización.

Para la instalación de paquetes de dispositivos, consulte Instalador de paquete de dispositivos: debe descargarse en la página 194.

Añadir/publicar componentes del instalador de Download Manager

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

Primero se añaden componentes nuevos y/o no estándar al Download Manager. A continuación, lo utiliza para afinar los componentes que deben estar disponibles en las distintas versiones lingüísticas de la página web.

Si el Download Manager está abierto, ciérrelo antes de instalar los nuevos componentes.

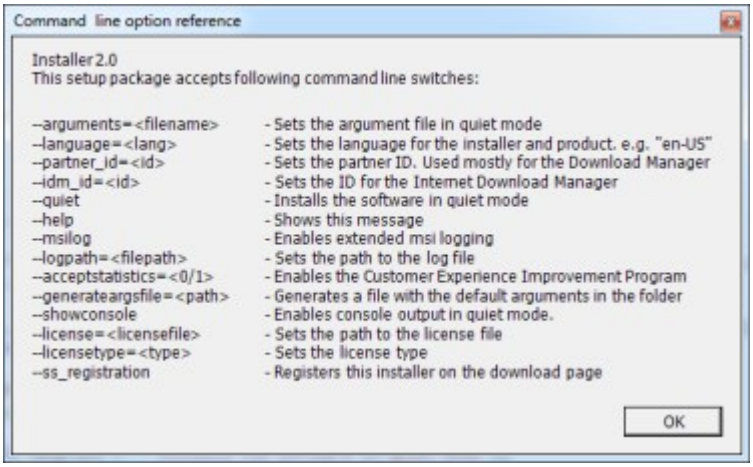
Añadir archivos nuevos/no estándar al Download Manager:

1. En el ordenador en el que ha descargado los componentes, vaya a **Inicio** de Windows introduzca un *Símbolo del sistema*
2. En el *Símbolo del sistema*, ejecute el nombre del archivo (*.exe*) con:[espacio]--*ss_registration*

   Ejemplo: *MilestoneXProtectRecordingServerInstaller_x64.exe --ss_registration*

   El archivo se añade ahora al Download Manager pero no se instala en el ordenador actual.

Para obtener una visión general de los comandos del instalador, en el *Símbolo del sistema,* introduzcacon:[espacio]--*help* y aparecerá la siguiente ventana:



Cuando se han instalado nuevos componentes, se seleccionan por defecto en el Download Manager y están inmediatamente disponibles para los usuarios a través de la página web. Siempre puede mostrar u ocultar características en la página web seleccionando o desmarcando casillas de verificación en la estructura de árbol del Download Manager.

Puede cambiar la secuencia en la que se muestran los componentes en la página web. En la estructura de árbol del Download Manager, arrastre los elementos del componente y suéltelos en la posición requerida.

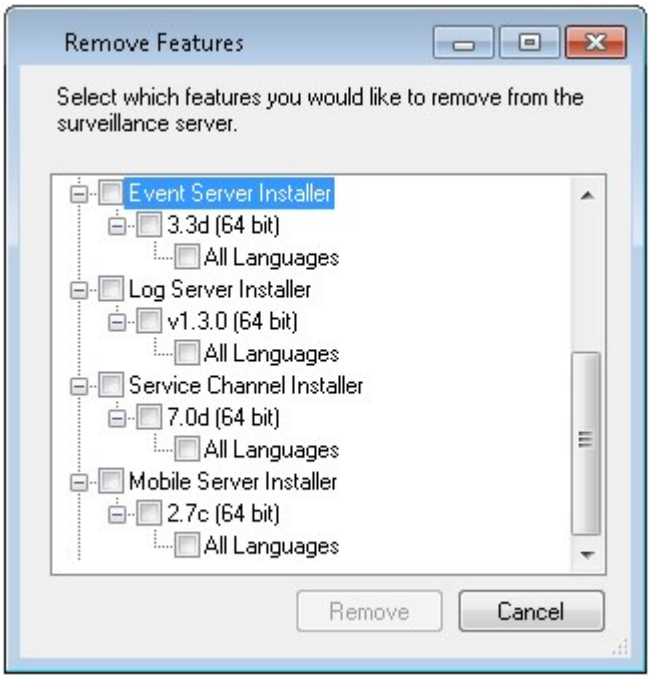
Ocultar/eliminar componentes del instalador Download Manager

Tiene tres opciones:

- **Oculte componentes** de la página web desmarcando las casillas de verificación en la estructura de árbol de Download Manager. Los componentes todavía están instalados en el servidor de gestión, y seleccionando las casillas de verificación en la estructura de árbol de Download Manager puede hacer que los componentes estén disponibles de nuevo rápidamente

- **Eliminar la instalación de componentes** en el servidor de gestión. Los componentes desaparecen de Download Manager, pero los archivos de instalación de los componentes se guardan 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 funciones**.
    2. En la ventana **Quitar funciones**, seleccione la(s) función(es) que desea quitar.



    3. Haga clic en **Aceptar** y en **Sí**.

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

Instalador de paquete de dispositivos: debe descargarse

El paquete de dispositivos (que contiene los controladores de dispositivos) incluido en su instalación original no está incluido en el Download Manager. Por lo tanto, si necesita reinstalar el paquete de dispositivos o hacer que el instalador del paquete de dispositivos esté disponible, en primer lugar debe añadir o publicar el último instalador del paquete de dispositivos en Download Manager:

1. Obtenga el último paquete de dispositivos regulares en la página de descargas del sitio web de Milestone (https://www.milestonesys.com/downloads/).
2. En la misma página, puede descargar el paquete de dispositivos heredados con controladores más antiguos. Para comprobar si sus cámaras utilizan controladores del paquete de dispositivos heredados, vaya a este sitio web (https://www.milestonesys.com/community/business-partner-tools/device-

packs/).

3. Añadirlo/publicarlo en el Download Manager llamándolo con el comando *--ss_registration*.

Si no tiene una conexión de red, puede reinstalar todo el servidor de grabación desde el Download Manager. Los archivos de instalación del servidor de grabación se colocan localmente en su ordenador y, de este modo, se obtiene automáticamente una reinstalación del paquete de dispositivos.

Archivos de registro de la instalación y solución de problemas

Durante una instalación, actualización o desinstalación, las entradas de registro se escriben en varios archivos de registro de instalación: Al archivo de registro de la instalación principal `installer.log` y a los archivos de registro pertenecientes a los diferentes componentes del sistema que está instalando. Todas las entradas de registro tienen una marca de tiempo y las más recientes se encuentran al final de los archivos de registro.

Puede encontrar todos los archivos de registro de la instalación en la carpeta `C:\ProgramData\Milestone\Installer\`. Los archivos de registro llamados *I.log o *I[integer].log son archivos de registro sobre nuevas instalaciones o actualizaciones, mientras que los archivos de registro llamados *U.log o *U[integer].log son sobre desinstalaciones. Si ha comprado un servidor con un sistema ya instalado XProtect a través de un socio de Milestone, es posible que no haya ningún archivo de registro de instalación.

Los archivos de registro contienen información sobre los parámetros de la línea de comandos y las opciones de la línea de comandos y sus valores utilizados durante una instalación, actualización o desinstalación. Para encontrar los parámetros de línea de comandos utilizados en los archivos de registro, busque **Línea de comandos:** o **Parámetro'** dependiendo del archivo de registro.

Para la resolución de problemas, el archivo principal de registro de la instalación installer.log es el primer lugar en el que hay que buscar. Si se produjo alguna excepción, error o advertencia durante la instalación, éstas se han registrado. Intente buscar una **excepción**, un **error** o una **advertencia**. "Código de salida": 0" significa una instalación exitosa y "Código de salida: 1" lo contrario. Sus hallazgos en los archivos de registro pueden permitirle encontrar una solución en la Milestone Base de conocimientos. Si no es así, póngase en contacto con su socio Milestone y comparta los archivos de registro de instalación correspondientes.

Configuración

Lista de tareas de configuración inicial

La siguiente lista de comprobación enumera las tareas iniciales para configurar su sistema. Algunas de ellas, puede que ya las haya completado durante la instalación.

Una lista de comprobación completa no garantiza por sí misma que el sistema se ajuste a los requisitos exactos de su organización. Para que el sistema se adapte a las necesidades de su organización, Milestone recomienda que lo supervise y lo ajuste continuamente.

Por ejemplo, es una buena idea probar y ajustar la configuración de la sensibilidad de la detección de movimiento de las cámaras individuales bajo diferentes condiciones físicas, incluyendo el día y la noche y el tiempo tranquilo y ventoso, una vez que el sistema está en funcionamiento.

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

Paso	Descripción
☑	Ha terminado la instalación inicial de su sistema. Consulte Instalar un nuevo sistema XProtect en la página 151.
☑	Cambie el SLC de prueba por un SLC permanente (si es necesario). Consulte Cambiar el código de licencia del software en la página 127.
☑	Inicie sesión en el Management Client. Consulte Iniciando sesión (explicación) en la página 28.
☐	Verifique que la configuración de almacenamiento de cada servidor de grabación se ajusta a sus necesidades. Consulte Almacenamiento y archivado (explicación) en la página 56.
☐	Verifique que la configuración de archivo de cada servidor de grabación se ajusta a sus necesidades. Consulte Propiedades de Ajustes de almacenamiento y grabación en la página 432.

Paso	Descripción
☐	Detecte el hardware, las cámaras o los codificadores de vídeo que debe añadir a cada servidor de grabación. Consulte Añadir hardware en la página 217.
☐	Configure las cámaras individuales de cada servidor de grabación. Consulte Cámaras (nodo Dispositivos) en la página 453.
☐	Permita 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 en la página 203.
☐	Habilite y configure los dispositivos. Consulte Dispositivos (nodo Dispositivos) en la página 449.
☐	Las reglas determinan en gran medida el comportamiento del sistema. Puede crear reglas para definir cuándo deben grabar las cámaras, cuándo deben patrullar las cámaras PTZ (pan-tilt-zoom) y cuándo deben enviarse las notificaciones, por ejemplo. Crear reglas. Consulte Reglas y eventos (explicación) en la página 79.
☐	Añade cometidos al sistema. Consulte Cometidos y permisos de un cometidos (explicación) en la página 69.
☐	Añade usuarios o grupos de usuarios a cada uno de los cometidos. Consulte Asignar/eliminar usuarios y grupos a/de roles en la página 296.
☐	Activar licencias. Consulte Activar licencias en línea en la página 125 o Activar licencias fuera de línea en la página 125.

Para obtener más información sobre cómo configurar el sistema en el panel **Navegación del sitio**, consulte Panel Navegación por el sitio en la página 395.

Servidores de grabación

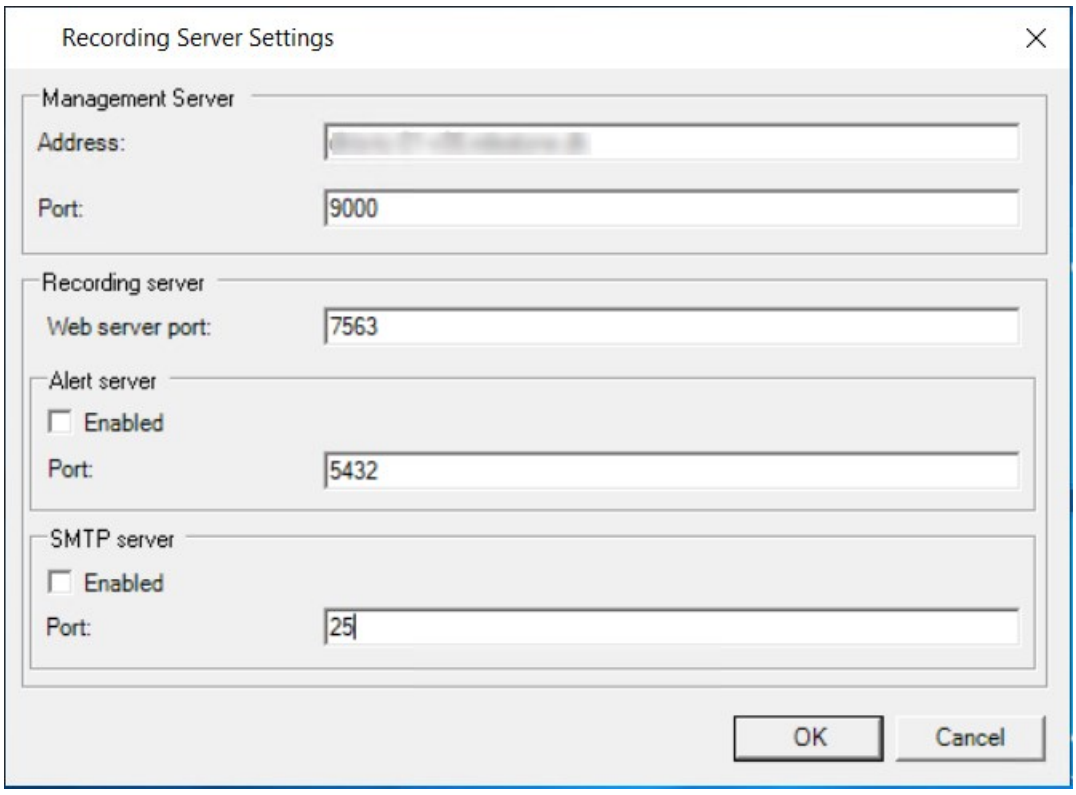
Cambiar o verificar la configuración básica de un servidor de grabación

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

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

1. En el ordenador que ejecuta el servidor de grabación, haga clic con el botón derecho en el icono del **Servidor de grabación** en el área de notificación.
2. Seleccione **Detener el servicio Recording Server**.
3. Vuelva a hacer clic con el botón derecho en el icono del **Servidor de grabación** y seleccione **Cambiar ajustes**.

   Aparece la ventana de **Ajustes del servidor de grabación**.



4. Verifique o cambie, por ejemplo, los siguientes ajustes:
    - **Servidor de gestión**: **Dirección**: Especifique la dirección IP o el nombre de host del servidor de gestión al que debe conectarse el servidor de grabación.
    - **Servidor de gestión**: **Puerto**: Especifique el número de puerto que se utilizará para comunicarse con el servidor de gestión. Puede cambiarlo si es necesario, pero el número de puerto debe coincidir siempre con el número de puerto configurado en el servidor de gestión. Consulte Puertos utilizados por el sistema en la página 99.
    - **Servidor de grabación**: **Puerto del servidor web**: Especifique el número de puerto que se utilizará cuando se comunique con el servidor web del servidor de grabación. Consulte Puertos utilizados por el sistema en la página 99.
    - **Servidor de grabación**: **Puerto del servidor de alertas**: Habilite y especifique el número de puerto que se utilizará cuando se comunique con el servidor de alertas del servidor de grabación, que escucha los mensajes de eventos de los dispositivos. Consulte Puertos utilizados por el sistema en la página 99.
    - **Servidor SMTP**: **Puerto**: Habilite y especifique el número de puerto que se utilizará cuando se comunique con el servicio de Protocolo simple de transferencia de correo (SMTP) del servidor de grabación. Consulte Puertos utilizados por el sistema en la página 99.
5. Haga clic en **Aceptar**.
6. Para volver a iniciar el servicio Recording Server, haga clic con el botón derecho en el icono del **Servidor de grabación** y seleccione **Iniciar servicio Recording Server**.

> ⚠ Detener el servicio Recording Server significa que no se puede grabar ni ver vídeo en directo mientras se verifica/cambia la configuración básica del servidor de grabación.

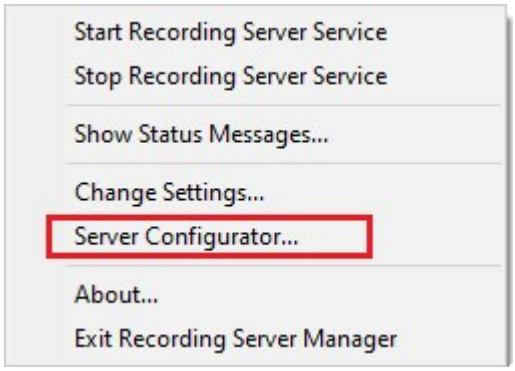
Registrar un servidor de grabación

Cuando instala un servidor de grabación, éste se registra automáticamente en la mayoría de los casos. Pero es necesario hacer el registro manualmente si:

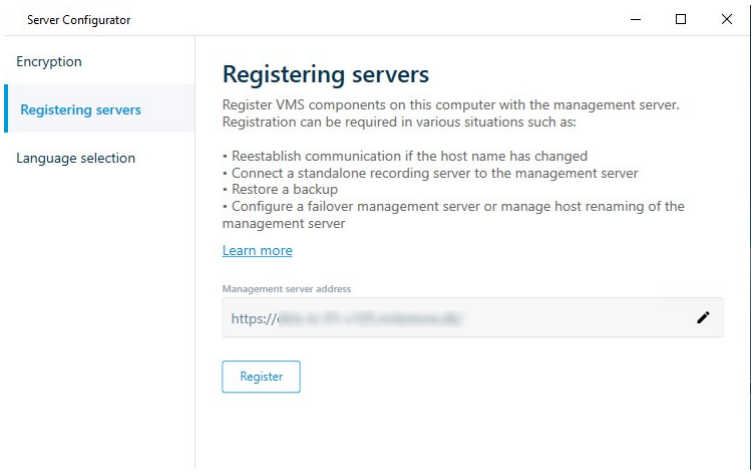
- Ha sustituido el servidor de grabación
- El servidor de grabación se instaló sin conexión y luego se añadió al servidor de gestión
- Su servidor de gestión no utiliza los puertos por defecto. Los números de puerto dependen de la configuración de cifrado. Si desea más información, consulte Puertos utilizados por el sistema en la página 99
- Un registro automático ha fallado, por ejemplo, después de cambiar la dirección del servidor de gestión, cambiar el nombre del ordenador con el servidor de grabación, o después de habilitar o deshabilitar los ajustes de cifrado de la comunicación con el servidor. Para obtener más información sobre los cambios en la dirección del servidor de gestión, consulte Cambiar el nombre del host del ordenador del servidor de gestión.

Al registrar un servidor de grabación, lo configurará para que se conecte a su servidor de gestión. La parte del servidor de gestión que se encarga del registro es el servicio Authorization Server.

1. Abra el Server Configurator dede el menú de inicio de Windows o desde el icono de la bandeja del servidor de grabación.



2. En el Server Configurator, seleccione **Registrando servidores**.



3. Verifique la dirección del servidor de gestión y el esquema (http o https) al que desea que se conecten los servidores del ordenador y haga clic en **Registrar**.

Aparece una confirmación que indica que el registro en el servidor de gestión se ha realizado con éxito.

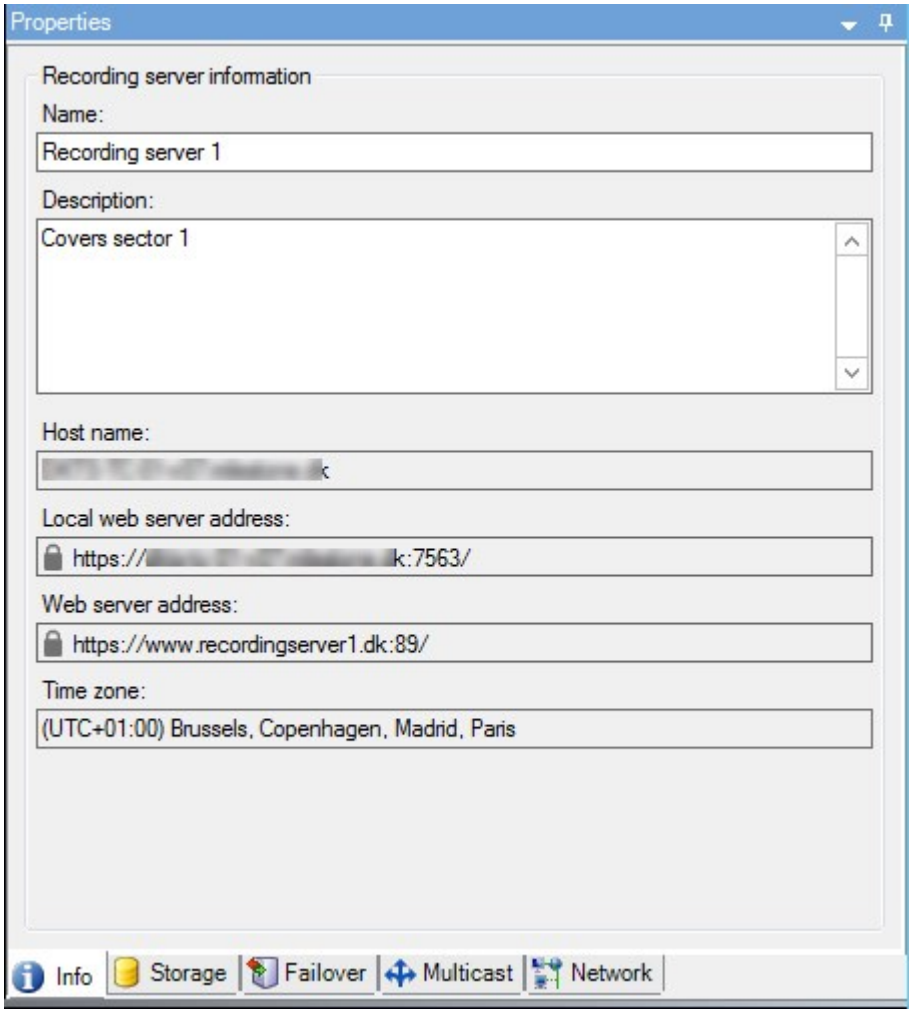
Consulte también Sustituir un servidor de grabación en la página 351.

Ver el estado del cifrado a los clientes

Para verificar si su servidor de grabación cifra las conexiones:

1. Abra el Management Client.
2. En el panel de **Navegación del sitio**, seleccione **Servidores** > **Servidores de grabación**. Esto abre una lista de servidores de grabación.

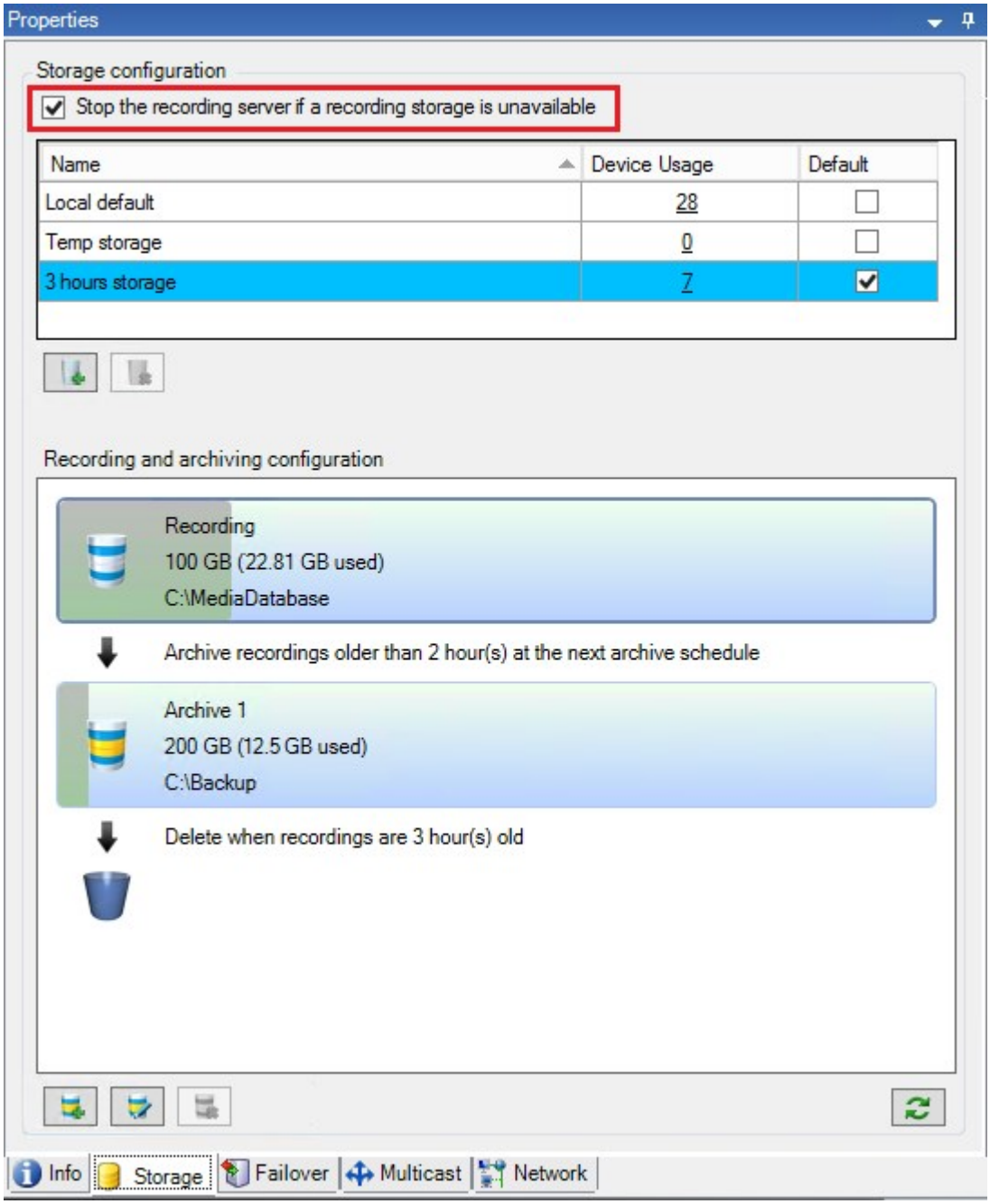
3. En el panel **Generalidades**, seleccione el servidor de grabación correspondiente y vaya a la pestaña de **Información**.
   Si se habilita el cifrado a los clientes y servidores que recuperan flujos de datos del servidor de grabación, aparecerá un icono de un candado delante de la dirección del servidor web local y de la dirección del servidor web opcional.



Especificar el comportamiento cuando el almacenamiento de la grabación no está disponible

Por defecto, el servidor de grabación sigue funcionando si un almacenamiento de grabación no está disponible. Si su sistema está configurado con servidores de grabación de failover, puede especificar el servidor de grabación que debe dejar de funcionar, para que los servidores de failover se hagan cargo:

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



Añadir un nuevo almacenamiento

Cuando se añade un nuevo almacenamiento, siempre se crea un almacenamiento de grabación con una base de datos de grabación predefinida llamada **Grabación**. No se puede renombrar la base de datos. Además del almacenamiento de grabaciones, un almacenamiento puede contener una serie de archivos.

1. Para añadir un almacenamiento adicional a un servidor de grabación seleccionado, haga clic en el botón  situado debajo de la lista de **Configuración de almacenamiento**. Se abre el cuadro de diálogo **Ajustes de almacenamiento y grabación**.
2. Especifique los ajustes pertinentes (consulte Propiedades de Ajustes de almacenamiento y grabación en la página 432).
3. Haga clic en **Aceptar**.

Si es necesario, ahora está listo para crear archivo(s) dentro de su nuevo almacenamiento.

Crear un archivo dentro de un almacenamiento

Un almacenamiento no tiene un archivo por defecto, pero se pueden crear archivos según sea necesario.

1. Seleccione el almacenamiento correspondiente en la lista **Configuración de grabaciones y archivos**.
2. Haga clic en el botón  debajo de la lista **Configuración de grabaciones y archivos**.
3. En el cuadro de diálogo **Ajustes del archivo**, especifique los ajustes necesarios (consulte Propiedades de ajustes de archivo en la página 434).
4. Haga clic en **Aceptar**.

Adjuntar un dispositivo o grupo de dispositivos a un almacenamiento

Una vez configurado un almacenamiento para un servidor de grabación, puede habilitarlo para dispositivos individuales como cámaras, micrófonos o altavoces o para un grupo de dispositivos. También puede seleccionar qué áreas de almacenamiento de un servidor de grabación desea utilizar para el dispositivo individual o el grupo.

1. Expanda los **Dispositivos** y seleccione **Cámaras**, **Micrófonos** o **Altavoces** según sea necesario.
2. Seleccione el dispositivo o un grupo de dispositivos.
3. Seleccione la pestaña **Grabar**.
4. En la zona de **Almacenamiento**, seleccione **Seleccionar**.
5. En el cuadro de diálogo que aparece, seleccione la base de datos que debe almacenar las grabaciones del dispositivo y luego haga clic en **Aceptar**.
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 pestaña Almacenamiento del servidor de grabación, el dispositivo es visible en el informe de mensajes que aparece.

Dispositivos deshabilitados

De forma predeterminada, los dispositivos deshabilitados no se muestran en el panel **Generalidades**.

Para mostrar todos los dispositivos deshabilitados, en la parte superior del panel **Generalidades**, haga clic en **Filtrar** para abrir la pestaña **Filtrar** y seleccione **Mostrar dispositivos deshabilitados**.

Para ocultar de nuevo los dispositivos deshabilitados, borre la selección de **Mostrar dispositivos deshabilitados**.

Editar los ajustes de un almacenamiento o archivo seleccionado

1. Para editar un almacenamiento, seleccione su base de datos de grabación en la lista de **Configuración de grabación y archivo**. Para editar un archivo, seleccione la base de datos del archivo.
2. Haga clic en el botón  **Editar almacenamiento de grabaciones** ubicado debajo de la lista **Configuración de grabaciones y archivos**.
3. Edite una base de datos de grabaciones o un archivo.

Si cambia el tamaño máximo de una base de datos, el sistema archiva automáticamente las grabaciones que superan el nuevo límite. Archiva automáticamente las grabaciones en el siguiente archivo o las elimina en función de la configuración del archivo.

Habilitar la firma digital para la exportación

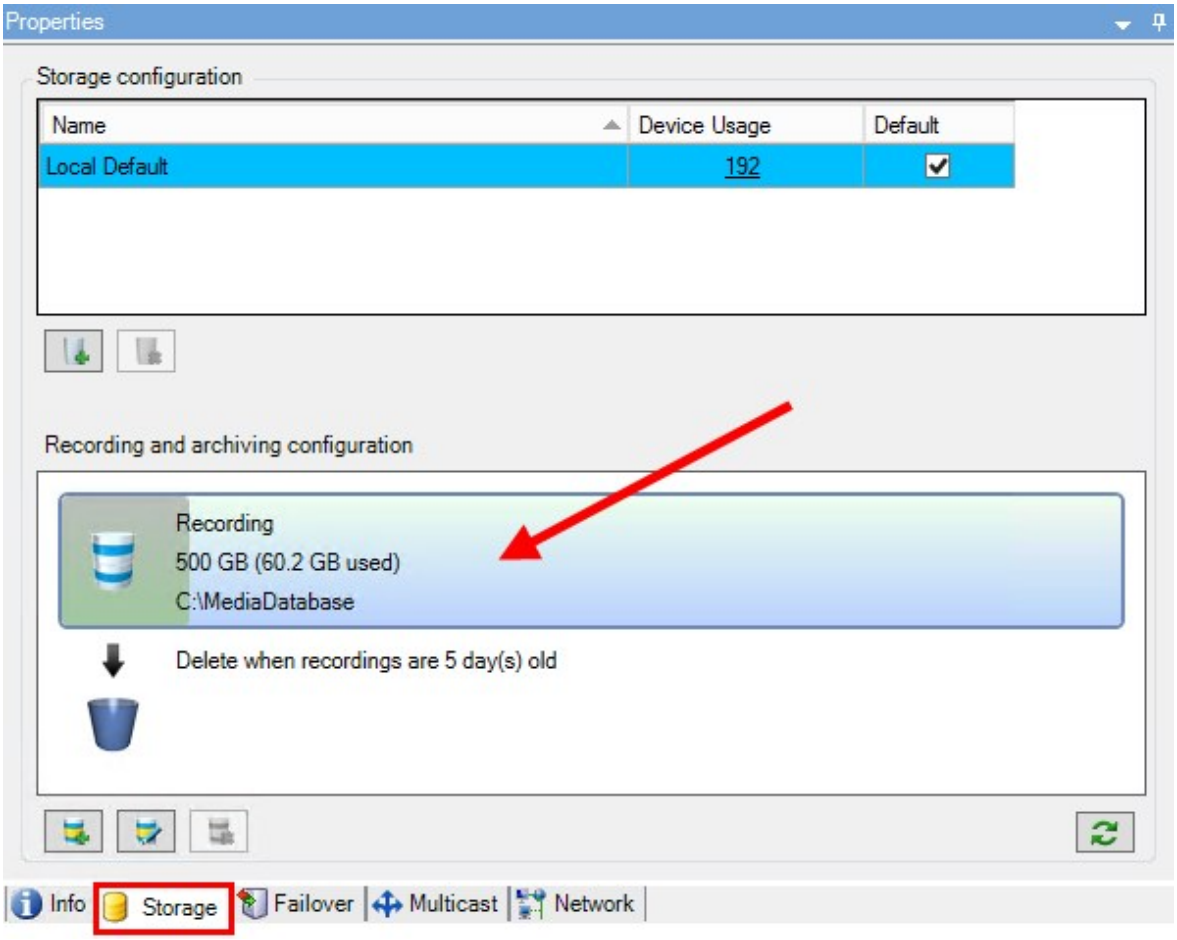
La funcionalidad disponible depende del sistema que esté utilizando. Vea la lista completa de características, que está disponible en la página de descripción del producto en el sitio web Milestone (https://www.milestonesys.com/solutions/platform/product-index/).

Puede habilitar la firma digital para el vídeo grabado, de modo que los usuarios clientes puedan verificar que el vídeo grabado no ha sido manipulado desde que se grabó. La verificación de la autenticidad del vídeo es algo que el usuario hace en XProtect Smart Client – Player después de exportar el vídeo.

La firma también debe estar activada en la pestaña XProtect Smart Client > **Exportaciones** > **Ajustes de exportación** > **formato XProtect** > **Incluir firma digital**. 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 generalidades, haga clic en el servidor de grabación para el que desea habilitar la firma.

4. En la parte inferior del panel de **Propiedades**, haga clic en la pestaña **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 de **Ajustes de almacenamiento y grabación**.
6. Seleccione la casilla de verificación **Firma**.
7. Haga clic en **Aceptar**.

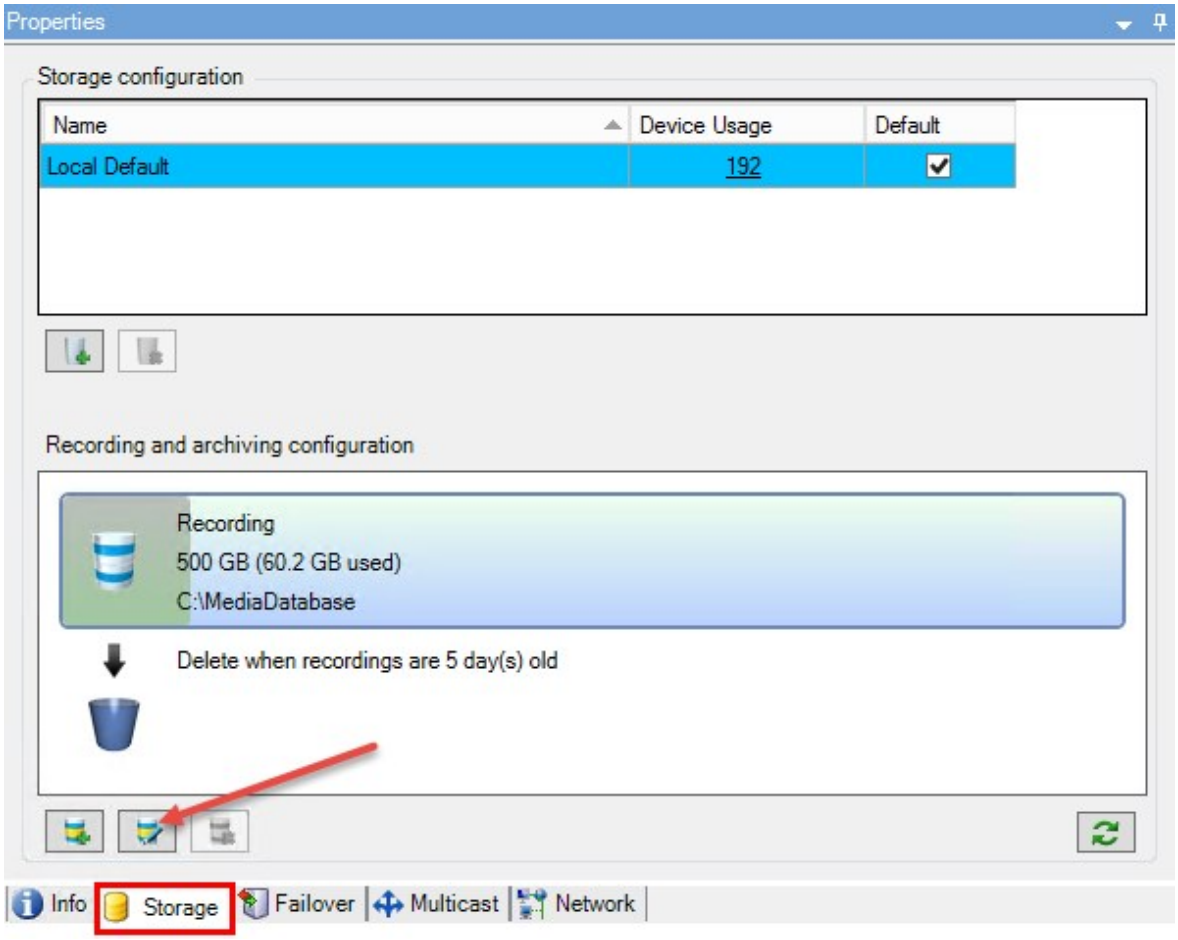
Cifrar sus grabaciones

La funcionalidad disponible depende del sistema que esté utilizando. Vea la lista completa de características, que está disponible en la página de descripción del producto en el sitio web Milestone (https://www.milestonesys.com/solutions/platform/product-index/).

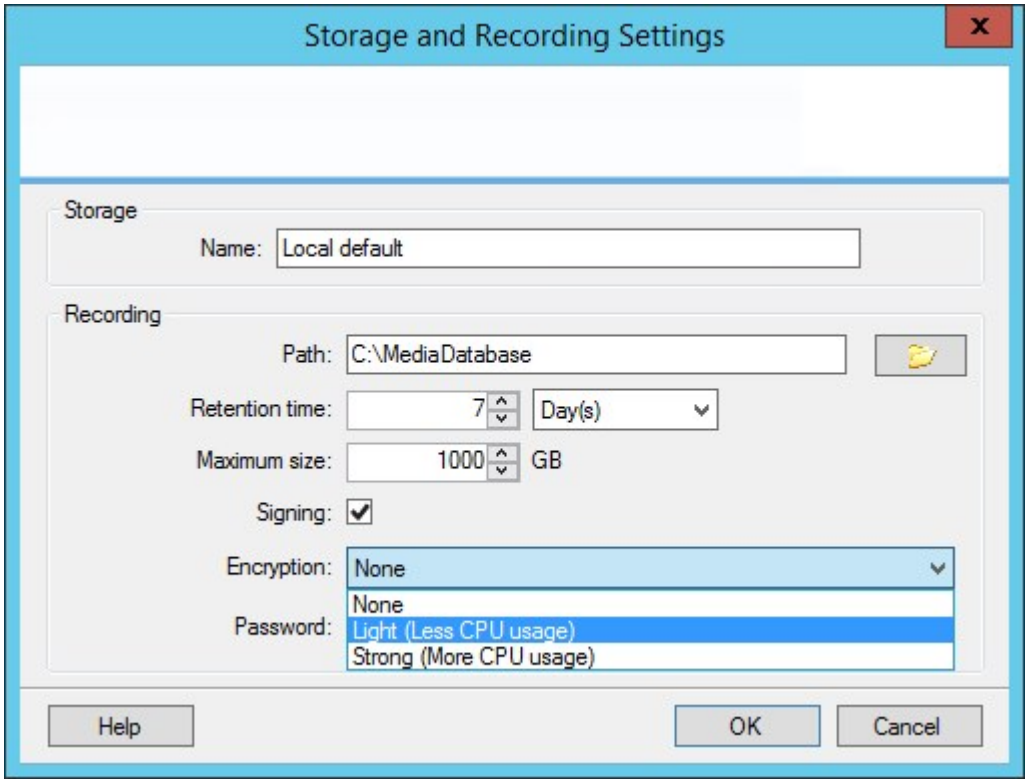
Puede asegurar sus grabaciones habilitando el cifrado en el almacenamiento y los archivos de sus servidores de grabación. Puede elegir entre un cifrado ligero o fuerte. Cuando habilite el cifrado, deberá especificar también una contraseña relacionada.

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

1. Haga clic en el botón **Editar almacenamiento de grabaciones** debajo de la lista **Configuración de grabaciones y archivos**.



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



3. Se le dirigirá automáticamente al cuadro de diálogo **Establecer contraseña**. Introduzca la contraseña y haga clic en **Aceptar**.

Hacer una copia de seguridad de las grabaciones archivadas

Muchas organizaciones quieren hacer copias de seguridad de sus grabaciones utilizando unidades de cinta o similares. La forma exacta de hacerlo es muy individual y depende de los medios de copia de seguridad utilizados en su organización. No obstante, conviene tener en cuenta lo siguiente:
Hacer copias de seguridad de los archivos en vez de las bases de datos de las cámaras

Cree siempre copias de seguridad basadas en el contenido de los archivos, no en las bases de datos individuales de las cámaras. Si crea copias de seguridad basadas en el contenido de las bases de datos de las cámaras individuales, puede provocar violaciones de la compartición u otros problemas de funcionamiento.

Cuando programe una copia de seguridad, asegúrese de que el trabajo de copia de seguridad no se solapa con los tiempos de archivo especificados. Para ver la programación de archivo de cada servidor de grabación en cada una de las áreas de almacenamiento de un servidor de grabación, consulte la pestaña Almacenamiento.
Conozca la estructura de su archivo para poder dirigirse a las copias de seguridad

Cuando se archivan las grabaciones, se guardan en una determinada estructura de subdirectorios dentro del archivo.

Durante todo el uso regular de su sistema, la estructura de subdirectorios es completamente transparente para los usuarios del sistema cuando navegan por las grabaciones con XProtect Smart Client. Esto es cierto tanto con las grabaciones archivadas como con las no archivadas. Es relevante conocer la estructura de los subdirectorios (consulte Estructura del archivo (explicación) en la página 61 si quiere hacer una copia de seguridad de sus grabaciones archivadas (consulte Hacer una copia de seguridad y restaurar la configuración del sistema en la página 340).

Eliminar un archivo de un almacenamiento

1. Seleccione el archivo desde la lista **Configuración de grabaciones y archivos**.

   Solo es posible eliminar el último archivo de la lista. El archivo no tiene que estar vacío.

2. Haga clic en el botón  ubicado debajo de la lista **Configuración de grabaciones y archivos**.
3. Haga clic en **Sí**.

   En el caso de los archivos no disponibles, por ejemplo, los archivos offline, no es posible verificar si el archivo contiene medios con bloqueos de evidencias, pero el archivo puede eliminarse si lo confirma el usuario.

   Los archivos disponibles (archivos online) que contienen medios con bloqueos de evidencias no se pueden eliminar.

Eliminar un almacenamiento

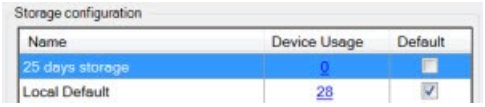
No puede eliminar el almacenamiento predeterminado o los almacenamientos que los dispositivos utilizan como almacenamiento de grabación para las grabaciones en directo.
Esto significa que es posible que tenga que trasladar los dispositivos (consulte Mover el hardware en la página 352) y las grabaciones aún no archivadas a otro almacenamiento antes de eliminarlo.

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 dispositivos que han sido trasladados a otro servidor de grabación, aparece una advertencia. Haga clic en el enlace para ver la lista de dispositivos.

2. Siga los pasos en Mover grabaciones no archivadas de un almacenamiento a otro en la página 209.

3. Continúe hasta que haya movido todos los dispositivos.
4. Seleccione el almacenamiento que desea eliminar.



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

Mover grabaciones no archivadas de un almacenamiento a otro

Las grabaciones se mueven de una base de datos de grabaciones en directo a otra desde la pestaña **Grabar** del dispositivo.

1. Seleccione el tipo de dispositivo. En el panel **Generalidades**, seleccione el dispositivo.
2. Haga clic en la pestaña **Grabar**. 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 **Aceptar**.
5. En el cuadro de diálogo **Acción de grabaciones**, seleccione si desea eliminar las grabaciones ya existentes, pero **no archivadas**, al nuevo almacenamiento o si desea eliminarlas.
6. Haga clic en **Aceptar**.

Asignar servidores de grabación failover

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

- Sin configuración de failover
- Una configuración de failover primaria/secundaria (espera en frío)
- Una configuración de espera en caliente

Si selecciona **b** y **c**, debe seleccionar el servidor/grupos específicos. Con **b**, también puede seleccionar un grupo de failover secundario. Si el servidor de grabación no está disponible, un servidor de grabación de failover del grupo primario de failover se hace cargo. Si también ha seleccionado un grupo de failover secundario, un servidor de grabación de failover del grupo secundario se hace cargo en caso de que todos los servidores de grabación de failover del grupo de failover primario estén ocupados. De este modo, solo se arriesga a no tener una solución de failover en el raro caso de que todos los servidores de grabación de 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 deseado, vaya a la pestaña **Failover**.
3. Para elegir el tipo de configuración de failover, seleccione entre:
   - **Ninguno**
   - **Grupo de servidores primarios de failover/Grupo de servidores secundarios de failover**
   - **Servidor de espera en caliente**

   No se puede seleccionar el mismo grupo de failover como grupo de failover primario y secundario ni seleccionar servidores regulares de failover que ya formen parte de un grupo de failover como servidores de espera en caliente.
4. A continuación, haga clic en **Ajustes avanzados de failover**. Esto abre la ventana de **Ajustes avanzados de failover**, con una lista de todos los dispositivos conectados al servidor de grabación seleccionado. Si ha seleccionado **Ninguno**, los ajustes avanzados de failover también están disponibles. El sistema guarda cualquier selección para posteriores configuraciones de failover.
5. Para especificar el nivel de soporte de failover, seleccione **Soporte completo**, **Solo en directo** o **Desactivado** para cada dispositivo de la lista. Haga clic en **Aceptar**.
6. En el campo **Puerto de comunicación del servicio de failover (TCP)**, edite el número de puerto si es necesario.

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

Habilitar la multidifusión para el servidor de grabación

En la comunicación de red normal, cada paquete de datos se envía desde un único emisor a un único destinatario, un proceso conocido como unidifusión. Pero con la multidifusión se puede enviar un solo 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 utilice la **multidifusión**, solo se necesita un flujo de datos en cada segmento de la red

La multidifusión, tal y como se describe aquí, **no** es una transmisión de vídeo de la cámara a los servidores, sino de los servidores a los clientes.

Con la multidifusión, trabaja con un grupo definido de destinatarios, basándose en opciones como los rangos de direcciones IP, la capacidad de habilitar/deshabilitar la multidifusión para cámaras individuales, la capacidad de definir el mayor tamaño de paquete de datos aceptable (MTU), el número máximo de enrutadores entre los que debe reenviarse un paquete de datos (TTL), etc.

> Los flujos de multidifusión no están cifrados, aunque el servidor de grabación utilice el cifrado.

La multidifusión no debe confundirse con la **retransmisión**, que envía datos a todas las personas conectadas a la red, aunque los datos quizá no sean relevantes para todos:

Nombre	Descripción
Unidifusión	Envía datos desde una única fuente a un único destinatario.
Multidifusión	Envía datos desde una única fuente a múltiples destinatarios dentro de un grupo claramente definido.
Retransmisión	Envía datos desde una única fuente a todos los integrantes de una red. Por lo tanto, la retransmisión puede ralentizar considerablemente la comunicación en la red.

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

- En la pestaña **Multidifusión**, seleccione la casilla **Multidifusión**

Si todo el rango de direcciones IP para la multidifusión ya está en uso en uno o más servidores de grabación, deberá liberar primero algunas direcciones IP de multidifusión antes de habilitar la multidifusión en otros servidores de grabación.

> Los flujos de multidifusión no están cifrados, aunque el servidor de grabación utilice el cifrado.

Habilitar la multidifusión para cámaras individuales

La multidifusión solo funciona cuando se habilita para las cámaras correspondientes:

1. Seleccione el servidor de grabación y seleccione la cámara deseada en el panel **Generalidades**.
2. En la pestaña **Cliente**, seleccione la casilla **Multidifusión en directo**. Repita la operación para todas las cámaras pertinentes.

Los flujos de multidifusión no están cifrados, aunque el servidor de grabación utilice el cifrado.

Definir la dirección pública y el puerto

Si necesita acceder al VMS con XProtect Smart Client a través de una red pública o no fiable, Milestone le recomienda que utilice una conexión segura a través de VPN. Esto ayuda a garantizar que la comunicación entre XProtect Smart Client y el servidor VMS está protegida.

Define una dirección IP pública del servidor de grabación en la pestaña **Red**.

¿Por qué utilizar una dirección pública?

Los clientes pueden conectarse tanto desde la red local como desde Internet, y en ambos casos el sistema de vigilancia debe proporcionar las direcciones adecuadas para que los clientes puedan acceder al vídeo en directo y al grabado desde los servidores de grabación:

- Cuando los clientes se conectan localmente, el sistema de vigilancia debe responder con direcciones y números de puerto locales
- Cuando los clientes se conectan desde Internet, el sistema de vigilancia debe responder con la dirección pública del servidor de grabación. Es la dirección del cortafuegos o del router NAT (Network Address Translation), y a menudo también un número de puerto diferente. La dirección y el puerto pueden entonces ser reenviados a la dirección y el puerto locales del servidor.

1. Para habilitar el acceso público, seleccione la casilla **Habilitar acceso público**.
2. Defina la dirección pública del servidor de grabación. Introduzca la dirección del cortafuegos o del router NAT para que los clientes que accedan al sistema de vigilancia desde Internet puedan conectarse a los servidores de grabación.
3. Especifique un número de puerto público. Siempre es conveniente que los números de puerto utilizados en el cortafuegos o en el router NAT sean diferentes de los utilizados localmente.

Si utiliza el acceso público, configure el cortafuegos o el router NAT para que las solicitudes enviadas a la dirección y el puerto públicos se reenvíen a la dirección y el puerto locales de los servidores de grabación correspondientes.

Asignar rangos de IP locales

Define una lista de rangos de IP locales que el sistema de vigilancia debe reconocer como procedentes de una red local:

- En la pestaña **Red**, haga clic en **Configurar**

Filtrar el árbol de dispositivos

El árbol de dispositivos en el panel **Generalidades** puede llegar a ser muy grande si tiene muchos dispositivos registrados. Puede filtrar el árbol de dispositivos para localizar con más facilidad los dispositivos con los que quiere trabajar.

Al proporcionar términos de filtrado que son únicos para algunos dispositivos específicos, puede mostrar efectivamente solo esos dispositivos específicos.

Filtrar el árbol de dispositivos

- En la parte superior del panel **Generalidades**, haga clic en **Filtrar** para abrir la pestaña **Filtrar**.
- En el campo **Escribir aquí para filtrar dispositivos**, introduzca uno o varios criterios de filtrado y haga clic en **Aplicar filtro** para filtrar la lista de dispositivos.

Características de los criterios de filtrado

Los criterios de filtrado se aplican a los valores de los campos nombre de dispositivo, nombre abreviado de dispositivo, dirección de hardware (IP), ID de dispositivo e ID de hardware.

Las coincidencias de filtros parciales no se muestran al filtrar los valores de los campos ID de hardware e ID de dispositivo. Como resultado, debe definir el número de identificación completo y exacto cuando filtre por ID de hardware o ID de dispositivo.

Las coincidencias parciales del filtro se muestran para los valores de los campos nombre de dispositivo, nombre corto del dispositivo y dirección de hardware, por lo que el término de filtro "cámar" mostrará todos los dispositivos que contengan la palabra "cámara" en el nombre de dispositivo.

> Los criterios de filtrado no distinguen entre mayúsculas y minúsculas, por lo que usar "cámara" o "Cámara" como criterio de filtrado generará los mismos resultados.

Especificación de múltiples criterios de filtrado

Puede especificar múltiples criterios de filtrado y, de ese modo, reducir el filtrado del árbol de dispositivos. Cuando se aplica el filtro, todos los criterios de filtrado definidos se consideran unidos con Y, lo que significa que son acumulativos.

Por ejemplo, si ha introducido dos criterios de filtrado: “Cámara” y “Almacén”, la lista mostrará todos los dispositivos que contengan las palabras “Cámara” y “Almacén” en el nombre de dispositivo, pero no mostrará los dispositivos que contengan las palabras “Cámara” y “Aparcamiento” en el nombre de dispositivo ni se mostrarán los dispositivos que solo contengan la palabra "Cámara" en el nombre de dispositivo.

Elimine criterios de filtrado del campo de filtrado para ampliar su filtro si ha especificado un filtro demasiado restrictivo. El filtro se aplica automáticamente al árbol de dispositivos al eliminar los criterios de filtrado.

Restablecimiento del filtro

Si elimina todos los criterios de filtrado del campo de filtrado, el panel **Generalidades** se restablece y volverá a mostrar todos los dispositivos.

> También puede pulsar **F5** para restablecer el filtro y borrar la selección de la casilla de verificación **Mostrar dispositivos deshabilitados**.

Dispositivos deshabilitados

De forma predeterminada, los dispositivos deshabilitados no se muestran en el panel **Generalidades**.

Para mostrar todos los dispositivos deshabilitados, en la parte superior del panel **Generalidades**, haga clic en **Filtrar** para abrir la pestaña **Filtrar** y seleccione **Mostrar dispositivos deshabilitados**.

Para ocultar de nuevo los dispositivos deshabilitados, borre la selección de **Mostrar dispositivos deshabilitados**.

Servidores failover

Configurar y habilitar servidores de grabación por failover

> Si ha deshabilitado el servidor de grabación failover, debe habilitarlo para que pueda tomar el relevo de los servidores de grabación estándar.

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

1. En el panel de **Navegación del sitio**, seleccione **Servidores** > **Servidores Failover**. Esto abre una lista de servidores de grabación de failover instalados y grupos de failover.
2. En el panel **Generalidades**, seleccione el servidor de grabación de failover requerido.
3. Haga clic con el botón derecho y seleccione **Habilitado**. El servidor de grabación de failover está ahora habilitado.
4. Para editar las propiedades del servidor de grabación de failover, vaya a la pestaña de **Información**.

5. Cuando haya terminado, vaya a la pestaña **Red**. Aquí puede definir la dirección IP pública del servidor de grabación de failover y más. Esto es relevante si se utiliza NAT (Network Address Translation) y el reenvío de puertos. Para obtener más información, consulte la pestaña **Red** del servidor de grabación estándar.
6. En el panel de **Navegación del sitio**, seleccione **Servidores** > **Servidores de grabación**. Seleccione el servidor de grabación para el que desea el soporte de failover y asigne los servidores de grabación de failover (consulte Pestaña Failover (servidor de grabación) en la página 436).

Para ver el estado de un servidor de grabación failover, mantenga el ratón sobre el icono de la bandeja Failover Recording Server Manager en el área de notificación. Aparece una información sobre la herramienta que contiene el texto introducido en el campo Descripción del servidor de grabación de fallos. Esto puede ayudarle a determinar de qué servidor de grabación de failover está configurado para hacerse cargo.

El servidor de grabación de failover hace un ping al servidor de gestión de forma regular para verificar que está en línea y que puede solicitar y recibir la configuración de los servidores de grabación estándar cuando sea necesario. Si se bloquea el ping, el servidor de grabación de failover no podrá tomar el relevo de los servidores de grabación estándar.

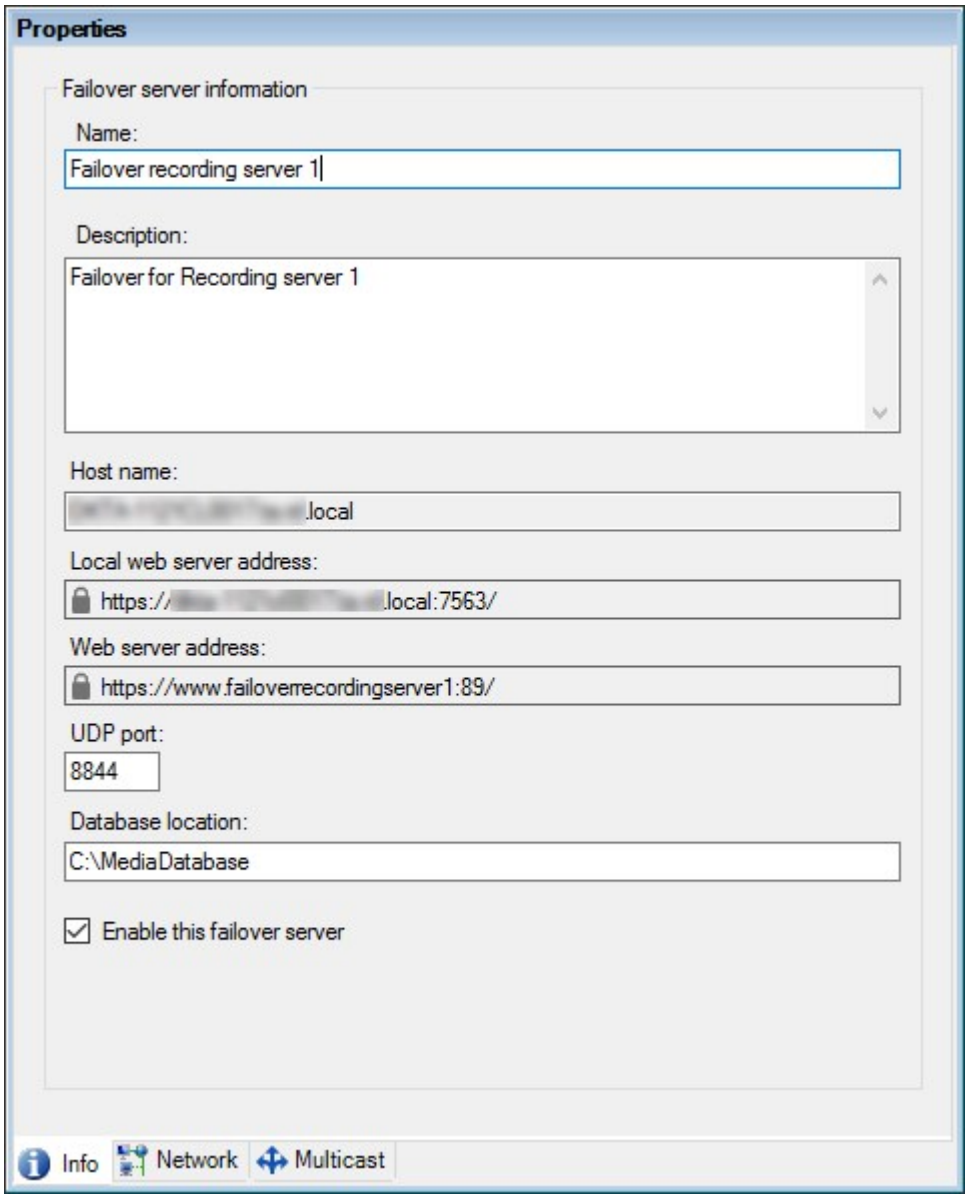
Servidores de grabación de failover en grupo para la espera en frío

1. Seleccione **Servidores** > **Servidores de Failover**. Esto abre una lista de servidores de grabación de failover instalados y grupos de failover.
2. En el panel **Generalidades**, haga clic con el botón derecho en los **Grupos de failover** del nodo superior y seleccione **Añadir grupo**.
3. Especifique un nombre (en este ejemplo *Grupo de Failover 1*) para y una descripción (opcional) de su nuevo grupo. Haga clic en **Aceptar**.
4. Haga clic con el botón derecho en el grupo (*Grupo de Failover 1*) que acaba de crear. Seleccione **Editar miembros de grupo**. De este modo, se abre la ventana **Seleccionar miembros del grupo**.
5. Arrastre y suelte o utilice los botones para mover los servidores de grabación de failover seleccionados del lado izquierdo al derecho. Haga clic en **Aceptar**. El(los) servidor(es) de grabación de failover seleccionado(s) pertenece(n) al grupo (*Grupo de Failover 1*) que acaba de crear.
6. Vaya a la pestaña **Secuencia**. Haga clic en **Arriba** y **Abajo** para establecer la secuencia interna de los servidores de registro de failover regulares en el grupo.

Ver el estado de cifrado en un servidor de grabación de failover

Para verificar si su servidor de grabación de failover utiliza el cifrado, haga lo siguiente:

1. En el panel de **Navegación del sitio**, seleccione **Servidores** > **Servidores Failover**. Esto abre una lista de servidores de grabación de failover.
2. En el panel **Generalidades**, seleccione el servidor de grabación correspondiente y vaya a la pestaña de **Información**.
   Si se habilita el cifrado a los clientes y servidores que recuperan flujos de datos del servidor de grabación, aparecerá un icono de un candado delante de la dirección del servidor web local y de la dirección del servidor web opcional.



Ver mensajes de estado

1. En el servidor de grabación de failover, haga clic con el botón derecho del ratón en el icono del **servicio Milestone Failover Recording Server**.
2. Seleccione **Mostrar mensajes de estado**. Aparece la ventana de **Mensajes de estado del servidor de failover**, con una lista de mensajes de estado con marca temporal.

Ver información de la versión

Conocer la versión exacta de su **servicio Failover Recording Server** es una ventaja si necesita ponerse en contacto con el servicio de asistencia del producto.

1. En el servidor de grabación de failover, haga clic con el botón derecho del ratón en el icono del **servicio Milestone Failover Recording Server**.
2. Seleccione **Acerca de**.
3. Se abre un pequeño cuadro de diálogo que muestra la versión exacta de su **servicio Failover Recording Server**.

Hardware

Añadir hardware

Tiene varias opciones para añadir hardware a cada servidor de grabación de su sistema.

> Si su hardware se encuentra detrás de un router con NAT o de un cortafuegos, es posible que tenga que especificar un número de puerto diferente y configurar el router/cortafuegos de forma que planifique el puerto y las direcciones IP que utiliza el hardware.

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

1. Para acceder a **Añadir hardware**, haga clic con el botón derecho del ratón en el servidor de grabación deseado y seleccione **Añadir hardware**.
2. Seleccione una de las opciones del asistente (consulte más abajo) y siga las instrucciones que aparecen en la pantalla.
3. Después de la instalación, puede ver el hardware y sus dispositivos en el panel de **Generalidades**.

> Algunos equipos deben ser preconfigurados al añadirlos por primera vez. Al añadir este tipo de hardware aparecerá un asistente adicional de **Preconfiguración de dispositivos de hardware**. Consultar Preconfiguración de hardware (explicación) en la página 52 para obtener más información.

Añadir hardware (diálogo)

El hardware representa o:

- 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
- Un servidor de grabación en un sitio remoto en una configuración Milestone Interconnect

Para obtener más información sobre cómo añadir hardware a su sistema, consulte Añadir hardware en la página 217.

Nombre	Descripción
Express (Recomendado)	El sistema busca automáticamente nuevo hardware en la red local del servidor de grabación. Seleccione la casilla **Mostrar el hardware que se ejecuta en otros servidores de grabación** para ver si el hardware detectado se ejecuta en otros servidores de grabación. Puede seleccionar esta opción cada vez que añada un nuevo hardware a su red y quiera utilizarlo en su sistema. No puede utilizar esta opción para añadir sistemas remotos en los ajustes de Milestone Interconnect. Para añadir hardware HTTP y HTTPS, ejecute la detección **Express** con el botón de opción **HTTPS (seguro)** seleccionado y, a continuación, con el botón de opción **HTTP (no seguro)** seleccionado.
Exploración del rango de direcciones	El sistema escanea su red en busca de hardware relevante y sistemas remotos de Milestone Interconnect basados en sus especificaciones de: • nombres de usuario y contraseñas del hardware. No necesario si su hardware utiliza los nombres de usuario y contraseñas por defecto.

Nombre	Descripción
	• drivers • rangos IP (solo IPv4) • número de puerto (por defecto = 80) Puede seleccionar esta opción cuando solo quiera escanear una parte de su red, por ejemplo, cuando amplíe su sistema.
Manual	Especifique los detalles de cada hardware y de los sistemas remotos Milestone Interconnect por separado. Esta puede ser una buena opción si quiere añadir solo unas pocas piezas de hardware y conoce sus direcciones IP, nombres de usuario y contraseñas relevantes o si una cámara no admite la función de detección automática.
Conectar hardware remotamente	El sistema busca el hardware conectado a través de un servidor conectado remotamente. Puede utilizar esta opción si ha instalado servidores para, por ejemplo, la conexión de cámaras Axis One-click. No puede utilizar esta opción para añadir sistemas remotos en los ajustes de Milestone Interconnect.

Deshabilitar / habilitar el hardware

El hardware añadido está **habilitado** por defecto.

Puede ver si el hardware está habilitado o deshabilitado de esta manera:

Habilitado
Deshabilitado

Para deshabilitar el hardware añadido, por ejemplo, por motivos de licencia o rendimiento

1. Expanda el servidor de grabación, haga clic con el botón derecho del ratón en el hardware que desee desactivar.
2. Seleccione **Habilitado** para borrarlo o seleccionarlo.

Editar hardware

Haga clic con el botón derecho del ratón en el hardware añadido y seleccione **Editar hardware** para modificar la configuración de red y los ajustes de autenticación de usuario del hardware en Management Client.

Editar hardware (diálogo)

En el caso de algunos dispositivos de hardware, el cuadro de diálogo **Editar hardware** también permite aplicar los ajustes directamente al dispositivo de hardware.

Si se selecciona el botón de opción **Editar ajustes Management Client**, el cuadro de diálogo **Editar hardware** muestra los ajustes que Management Client utiliza para conectarse al hardware. Para asegurarse de que el dispositivo de hardware se añade al sistema correctamente, introduzca los mismos ajustes que utiliza para conectarse a la interfaz de configuración de hardware del fabricante:

Nombre	Descripción
Nombre	Muestra el nombre del hardware junto a su dirección IP detectada (entre paréntesis).
Hardware URL	La dirección web de la interfaz de configuración del hardware del fabricante, que suele contener la dirección IP del hardware. Especifique una dirección válida en su red.
Nombre de usuario	El nombre de usuario utilizado para conectarse al hardware. El nombre de usuario que introduzca aquí no cambia el nombre de usuario en el dispositivo de hardware real. Seleccione el botón de opción **Editar Management Client y ajustes de hardware** para modificar los ajustes en los dispositivos de hardware compatibles.
Contraseña	La contraseña utilizada para conectarse al hardware. La contraseña que introduzca aquí no cambia la contraseña del dispositivo de hardware real. Seleccione el botón de opción **Editar Management Client y ajustes de hardware** para modificar los ajustes en los dispositivos de hardware compatibles. Para obtener información sobre cómo cambiar las contraseñas en varios dispositivos de hardware, consulte Cambiar contraseñas en dispositivos de hardware en la página 225.

Nombre	Descripción
	Como administrador del sistema, debe dar permiso a otros usuarios para ver la contraseña en Management Client. Para obtener más información, consulte Ajustes de cometido en Hardware.

Si se selecciona el botón de opción **Editar Management Client y ajustes de hardware** (para el hardware compatible), el cuadro de diálogo **Editar hardware** muestra los ajustes que también se aplican directamente al dispositivo de hardware:

> La aplicación de la configuración con este botón de radio seleccionado sobrescribirá la configuración actual del dispositivo de hardware. El hardware perderá momentáneamente la conexión con el servidor de grabación mientras se aplican los ajustes.

Nombre	Descripción
Nombre	Muestra el nombre del hardware junto a su dirección IP detectada (entre paréntesis).
Configuración de red	La configuración de red del hardware. Para ajustar los ajustes de la red, seleccione Configurar en la página 221.
Configurar	Especifique el protocolo de Internet (para los dispositivos de hardware compatibles) utilizando la lista desplegable de la **versión IP**. • Para IPv4, los valores deben tener el formato: **(0-999).(0-999).(0-999).(0-999)** • Para IPv6, los valores deben estar en el formato de ocho grupos de dígitos hexadecimales, cada uno separado por dos puntos. La máscara de subred debe ser un número entre **0 y 128**. El botón **Comprobar** comprueba si hay actualmente otro dispositivo de hardware en el sistema que esté utilizando la dirección IP introducida. La **verificación** no puede detectar conflictos con dispositivos de hardware que estén apagados, fuera del sistema XProtect VMS o que no respondan momentáneamente.

Nombre	Descripción
Nombre de usuario	El nombre de usuario y el nivel utilizado para conectarse al hardware. Seleccione otro usuario de la lista desplegable y añada una nueva contraseña utilizando el campo **Contraseña** que se describe a continuación. Añadir o eliminar usuarios utilizando las acciones subrayadas en la parte inferior de la sección de **Autentificación** (consulte Añadir un usuario en la página 222 o Eliminar usuarios en la página 223). Seleccionar un usuario que no tenga el nivel de usuario más alto especificado por el fabricante podría hacer que algunas funciones no estén disponibles.
Contraseña	La contraseña utilizada para conectarse al hardware. Ver el texto introducido actualmente mediante el icono de **Revelar** . Cuando cambie la contraseña, consulte la documentación del fabricante para conocer las reglas de contraseña para el dispositivo de hardware específico, o utilice el icono **Generar contraseña** para generar automáticamente una contraseña que se ajuste a los requisitos. Para obtener información sobre cómo cambiar las contraseñas en varios dispositivos de hardware, consulte Cambiar contraseñas en dispositivos de hardware en la página 225. Como administrador del sistema, debe dar permiso a otros usuarios para ver la contraseña en Management Client. Para obtener más información, consulte Ajustes de cometido en Hardware.
Añadir un usuario	Seleccione el enlace subrayado **Añadir** para abrir el cuadro de diálogo **Añadir un usuario** y añadir un usuario al dispositivo de hardware. Añadir un usuario lo establecerá automáticamente como usuario activo y sobrescribirá las credenciales introducidas anteriormente.

Nombre	Descripción
	Cuando cree la contraseña, consulte la documentación del fabricante para conocer las reglas de la contraseña para el dispositivo de hardware específico, o utilice el icono **Generar contraseña** para generar automáticamente una contraseña que se ajuste a los requisitos. Se preseleccionará automáticamente el nivel de usuario más alto detectado en el dispositivo de hardware. No se recomienda modificar el **Nivel de usuario** de su valor por defecto. Seleccionar un **Nivel de usuario** que no sea el más alto especificado por el fabricante podría hacer que algunas funciones no estén disponibles.
Eliminar usuarios	Seleccione el enlace subrayado **Eliminar** para abrir el cuadro de diálogo **Eliminar usuarios** y eliminar los usuarios del dispositivo de hardware. No se puede eliminar el usuario actualmente activo. Para establecer un nuevo usuario, utilice el cuadro de diálogo **Añadir un usuario** descrito anteriormente y, a continuación, elimine el antiguo usuario mediante esta interfaz.

Habilitar/deshabilitar dispositivos individuales

Las **cámaras** están habilitadas **por defecto**.

Los micrófonos, los altavoces, los metadatos, las entradas y las **salidas** están **deshabilitados** por defecto.

Esto significa que los micrófonos, los altavoces, los metadatos, las entradas y las salidas deben habilitarse individualmente antes de poder utilizarlos en el sistema. El motivo es que los sistemas de vigilancia se basan en las cámaras, mientras que el uso de los micrófonos y demás es muy individualizado en función de las necesidades de cada organización.

Puede ver si los dispositivos están habilitados o deshabilitados (los ejemplos muestran una salida):

Deshabilitado
Habilitado

El mismo método para habilitar/deshabilitar se utiliza para las cámaras, micrófonos, altavoces, metadatos, entradas y salidas.

1. Expanda el servidor de grabación y el dispositivo. Haga clic con el botón derecho del ratón en el dispositivo que desee habilitar.
2. Seleccione **Habilitado** para borrarlo o seleccionarlo.

Configurar una conexión segura con el hardware

Puede configurar una conexión segura HTTPS utilizando 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 cárguelo en él, antes de continuar con los pasos siguientes:

1. En el panel **Generalidades**, haga clic con el botón derecho en el servidor de grabación y seleccione el hardware.

2. En la pestaña **Ajustes**, habilite HTTPS. Esto no está habilitado por defecto.
3. Introduzca el puerto del servidor de grabación al que se conecta la conexión HTTPS. El número de puerto debe coincidir con el puerto configurado en la página de inicio del dispositivo.
4. Realice los cambios necesarios y guárdelos.

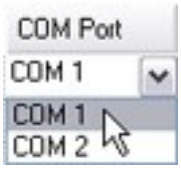
Habilitar la PTZ en un codificador de vídeo

Para habilitar el uso de cámaras PTZ en un codificador de vídeo, haga lo siguiente en la pestaña **PTZ**:

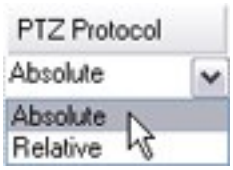
1. En la lista de dispositivos conectados al codificador de vídeo, seleccione la casilla **Habilitar PTZ** para las cámaras correspondientes:

2. En la columna **ID del dispositivo PTZ**, verifique el ID de cada cámara.

3. En la columna **Puerto COM**, seleccione los puertos COM (comunicaciones en serie) del codificador de vídeo que se utilizarán para el control de la funcionalidad PTZ:



4. En la columna **Protocolo PTZ**, seleccione el esquema de posicionamiento que desea utilizar:



   - **Absoluto**: Cuando los operadores utilizan los controles PTZ para la cámara, ésta se ajusta en relación con una posición fija, a menudo denominada posición inicial de la cámara
   - **Relativo**: Cuando los operadores utilizan los controles PTZ para la cámara, ésta se ajusta en relación con su posición actual

   El contenido de la columna del **protocolo PTZ** varía mucho en función del hardware. Algunos tienen de 5 a 8 protocolos diferentes. Consulte también la documentación de la cámara.

5. En la barra de herramientas, haga clic en **Guardar**.
6. Está a punto de configurar las posiciones preestablecidas y el patrullaje para cada cámara PTZ:
   - Añadir una posición preestablecida (tipo 1)
   - Añadir un perfil de patrulla

Cambiar contraseñas en dispositivos de hardware

> La funcionalidad disponible depende del sistema que esté utilizando. Vea la lista completa de características, que está disponible en la página de descripción del producto en el sitio web Milestone (https://www.milestonesys.com/solutions/platform/product-index/).

Puede cambiar las contraseñas de varios dispositivos de hardware en una sola operación.

Inicialmente, los dispositivos compatibles son modelos de Canon, Axis, Bosch, Hanwa, Panasonic, Sony, Hikvision y dispositivos de hardware compatibles con ONVIF, pero la interfaz de usuario le muestra directamente si un modelo es compatible o no. También puede acudir a nuestra página web para saber si un modelo es compatible: https://www.milestonesys.com/community/business-partner-tools/supported-devices/

> En el caso de los dispositivos que no admiten la gestión de contraseñas de dispositivos, debe cambiar la contraseña de un dispositivo de hardware desde su página web y luego introducir manualmente la nueva contraseña en Management Client. Si desea más información, consulte Editar hardware en la página 219.

Puede elegir:

- Deje que el sistema genere contraseñas individuales para cada dispositivo de hardware. El sistema genera contraseñas basadas en los requisitos del fabricante de los dispositivos de hardware.
- Utilice una sola contraseña definida por el usuario para todos los dispositivos de hardware. Al aplicar las nuevas contraseñas, los dispositivos de hardware pierden momentáneamente la conexión con el servidor de grabación. Después de aplicar las nuevas contraseñas, el resultado de cada dispositivo de hardware aparece en la pantalla. En el caso de cambios no exitosos, aparece el motivo del fallo si el dispositivo de hardware admite dicha información. Desde el asistente, puede crear un informe de los cambios de contraseña exitosos y fallidos, pero los resultados también se registran en **Registros del servidor**.

  > Para los dispositivos de hardware con controladores ONVIF y múltiples cuentas de usuario, solo un administrador de XProtect con permisos administrativos del dispositivo de hardware puede cambiar las contraseñas desde el VMS.

Requisitos:

- El modelo de dispositivo de hardware admite la gestión de la contraseña del dispositivo mediante Milestone.

Pasos:

1. En el panel **Navegación del sitio**, seleccione el nodo **Servidores de grabación**.
2. Haga clic con el botón derecho del ratón en el servidor de grabación o en el hardware correspondiente en el panel de visión general.
3. Seleccione **Cambiar contraseña de hardware**. Aparece un asistente.
4. Escriba la contraseña con letras minúsculas y mayúsculas, números y los siguientes caracteres: **! ( ) * - . _**

   La longitud máxima de la contraseña es de 64 caracteres.

   > La longitud máxima de la contraseña para la cámara Bosch FLEXIDOME IP outdoor NDN-50051 de 5000 MP es de 19 caracteres.

5. Siga las instrucciones de la pantalla para completar los cambios.

> El campo **Último cambio de contraseña** muestra la fecha y hora del último cambio de contraseña según la configuración de la hora local del ordenador desde el que se cambió la contraseña.

6. La última página muestra el resultado. Si el sistema no pudo actualizar una contraseña, haga clic en **Fallido** junto al dispositivo de hardware para ver el motivo.
7. También puede hacer clic en el botón **Imprimir informe** para ver la lista completa de actualizaciones exitosas y no exitosas.
8. En caso de que quiera cambiar la contraseña en los dispositivos de hardware que han fallado, haga clic en **Reintentar**, y el asistente comenzará de nuevo con los dispositivos de hardware que han fallado.

> Si selecciona **Reintentar**, ya no podrá acceder al informe de la primera vez que completó el asistente.

> Debido a las restricciones de seguridad, algunos dispositivos de hardware podrían dejar de estar disponibles durante un cierto tiempo si no se cambia la contraseña varias veces seguidas. Las restricciones de seguridad varían según los distintos fabricantes.

Actualizar el firmware de los dispositivos de hardware

> La funcionalidad disponible depende del sistema que esté utilizando. Vea la lista completa de características, que está disponible en la página de descripción del producto en el sitio web Milestone (https://www.milestonesys.com/solutions/platform/product-index/).

Management Client le permite actualizar el firmware del hardware que se ha añadido a su sistema VMS. Puede actualizar el firmware de varios dispositivos de hardware simultáneamente si son compatibles con el mismo archivo de firmware.

La interfaz de usuario le muestra directamente si un modelo admite actualizaciones de firmware. También puede ir al sitio web de Milestone para saber si un modelo es compatible: https://www.milestonesys.com/community/business-partner-tools/supported-devices/

En el caso de los dispositivos que no admiten actualizaciones de firmware, deberá actualizar el firmware de un dispositivo de hardware desde su página web.

Cuando se actualiza el firmware, los dispositivos de hardware pierden momentáneamente la conexión con el servidor de grabación.

Después de actualizar el firmware, el resultado de cada dispositivo de hardware aparece en la pantalla. En el caso de cambios no exitosos, aparece el motivo del fallo si el dispositivo de hardware admite dicha información. Los resultados también se registran en **Registros del servidor**.

Para los dispositivos de hardware con controladores ONVIF y múltiples cuentas de usuario, solo un administrador de XProtect con permisos administrativos del dispositivo de hardware puede actualizar el firmware desde el VMS.

Requisitos:

- El modelo de dispositivo de hardware admite la actualización del firmware mediante Milestone.

Pasos:

1. En el panel **Navegación del sitio**, seleccione el nodo **Servidores de grabación**.
2. Haga clic con el botón derecho del ratón en el servidor de grabación o en el hardware correspondiente en el panel de visión general.
3. Seleccione **Actualizar firmware de hardware**. Aparece un asistente.
4. Siga las instrucciones de la pantalla para completar los cambios.

   Solo puede actualizar varios dispositivos de hardware que sean compatibles con el mismo archivo de firmware. El hardware que se añade a través del controlador ONVIF se encuentra bajo **otro**, en lugar de su nombre de fabricante.

6. La última página muestra el resultado. Si el sistema no pudo actualizar el firmware, haga clic en **Fallido** junto al dispositivo de hardware para ver el motivo.

Milestone no se hace responsable del mal funcionamiento del dispositivo de hardware si se selecciona un archivo de firmware o un dispositivo de hardware incompatible.

Añadir y configurar un IDP externo

1. En Management Client, seleccione **Herramientas** > **Opciones** y abra la pestaña **IDP externo**.
2. En la sección **IDP externo**, seleccione **Añadir**.
3. Introduzca la información del IDP externo. Para obtener más información sobre la información necesaria, consulte IDP externo.

Para obtener información sobre cómo registrar las reclamaciones del IDP externo que desea utilizar en el VMS, consulte Registrar reclamaciones de un IDP externo.

Detalles de interfaz de usuario

Añadir un grupo de dispositivos

1. En el panel **Generalidades**, haga clic con el botón derecho en el tipo de dispositivo bajo el que desea crear un grupo de dispositivos.
2. Seleccione **Añadir grupo de dispositivos**.
3. En el cuadro de diálogo **Añadir grupo de dispositivos**, especifique un nombre y una descripción del nuevo grupo de dispositivos:

   La descripción aparece cuando se detiene el puntero del ratón sobre el grupo de dispositivos en la lista de grupos de dispositivos.
4. Haga clic en **Aceptar**. En la lista aparece una carpeta que representa el nuevo grupo de dispositivos.
5. Continúe especificando qué dispositivos incluir en un grupo de dispositivos (consulte Especificar qué dispositivos incluir en un grupo de dispositivos en la página 229).

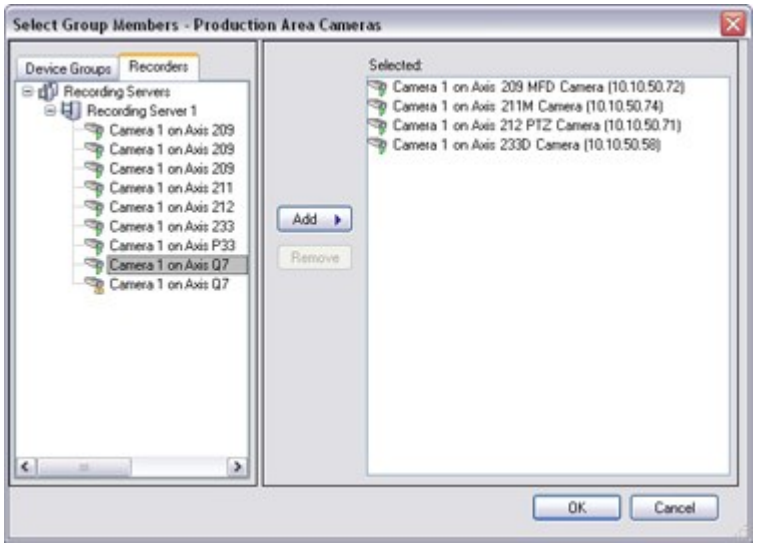
Especificar qué dispositivos incluir en un grupo de dispositivos

1. En el panel **Descripción general**, haga clic con el botón derecho en la carpeta de grupos de dispositivos relevante.
2. Seleccione **Editar miembros del grupo de dispositivos**.

3. En la ventana **Seleccionar miembros del grupo**, seleccione una de las pestañas para localizar el dispositivo.

   Un dispositivo puede ser un miembro de uno o varios grupos de dispositivos.

4. Seleccione los dispositivos que quiere incluir y haga clic en **Añadir** o haga doble clic en el dispositivo:



5. Haga clic en **Aceptar**.

6. Si supera el límite de 400 dispositivos en un grupo, puede añadir grupos de dispositivos como subgrupos en otros grupos de dispositivos:

Dispositivos deshabilitados

De forma predeterminada, los dispositivos deshabilitados no se muestran en el panel **Generalidades**.

Para mostrar todos los dispositivos deshabilitados, en la parte superior del panel **Generalidades**, haga clic en **Filtrar** para abrir la pestaña **Filtrar** y seleccione **Mostrar dispositivos deshabilitados**.

Para ocultar de nuevo los dispositivos deshabilitados, borre la selección de **Mostrar dispositivos deshabilitados**.

Especificar propiedades comunes para todos los dispositivos de un grupo de dispositivos

Con grupos de dispositivos, puede especificar propiedades comunes para todos los dispositivos de un grupo de dispositivos determinado:

1. En el panel **Descripción general**, haga clic en el grupo de dispositivos.

   En el panel **Propiedades**, todas las propiedades **que están disponibles en todos los dispositivos del grupo de dispositivos** se enumeran y se agrupan en pestañas.

2. Especifique las propiedades comunes relevantes.

   En la pestaña **Ajustes**, puede cambiar entre ajustes para **todos** los dispositivos y ajustes para 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.

Dispositivos deshabilitados

De forma predeterminada, los dispositivos deshabilitados no se muestran en el panel **Generalidades**.

Para mostrar todos los dispositivos deshabilitados, en la parte superior del panel **Generalidades**, haga clic en **Filtrar** para abrir la pestaña **Filtrar** y seleccione **Mostrar dispositivos deshabilitados**.

Para ocultar de nuevo los dispositivos deshabilitados, borre la selección de **Mostrar dispositivos deshabilitados**.

Habilitar/deshabilitar dispositivos mediante grupos de dispositivos

Solo puede habilitar/deshabilitar los dispositivos a través del hardware configurado. A menos que se habilite/deshabilite manualmente en el asistente de adición de hardware, los dispositivos de cámara están habilitados por defecto y todos los demás dispositivos están deshabilitados por defecto.

De forma predeterminada, los dispositivos deshabilitados no se muestran en el panel **Generalidades**.

Para mostrar todos los dispositivos deshabilitados, en la parte superior del panel **Generalidades**, haga clic en **Filtrar** para abrir la pestaña **Filtrar** y seleccione **Mostrar dispositivos deshabilitados**.

Para ocultar de nuevo los dispositivos deshabilitados, borre la selección de **Mostrar dispositivos deshabilitados**.

Para ubicar un dispositivo a través de los grupos de dispositivos para habilitar o deshabilitar:

1. En el panel **Navegación del sitio**, seleccione el dispositivo.
2. En el panel **Generalidades**, expanda el grupo correspondiente y busque el dispositivo.
3. Haga clic con el botón derecho en el dispositivo y seleccione **Ir a hardware**.
4. Haga clic en el nodo más para ver todos los dispositivos del hardware.
5. Haga clic con el botón derecho en el dispositivo que desea habilitar/deshabilitar y seleccione **Habilitado**.

Dispositivos - Ajustes de cámara

Ver o editar ajustes de la cámara

1. En el panel **Navegación del sitio**, seleccione **Dispositivos** y a continuación seleccione **Cámaras**.
2. Seleccione la cámara correspondiente en el panel **Generalidades**.
3. Abra la pestaña **Ajustes**.

Puede ver o editar ajustes, como:

- Velocidad de fotogramas predeterminada
- Resolución
- Compresión
- El número máximo de fotogramas entre fotogramas clave
- Visualización de fecha/hora/texto en pantalla para una cámara seleccionada o para todas las cámaras dentro de un grupo de dispositivos

Los controladores para las cámaras determinan el contenido de la pestaña **Ajustes**. Los controladores varían dependiendo del tipo de cámara.

Para cámaras que admitan más de un tipo de flujo, por ejemplo, MJPEG y MPEG-4/H.264/H.265, puede usar flujos de datos múltiples, consulte Gestionar la transmisión múltiple en la página 239.

Previsualizar

Cuando cambia un ajuste, puede verificar rápidamente el efecto del cambio si tiene el panel **Vista previa** habilitado.

- Para habilitar **Vista previa**, haga clic en el menú **Ver** y luego haga clic en **Ventana de vista previa**.

No puede utilizar el panel **Vista previa** para juzgar el efecto de los cambios en la velocidad de fotogramas porque las imágenes en miniatura del panel **Vista previa** utilizan otra velocidad de fotogramas que se define en el cuadro de diálogo **Opciones**.

Rendimiento

Si cambia los ajustes para **Número máximo de fotogramas entre fotogramas clave** y **Modo número máximo de fotogramas ente fotogramas clave**, puede ralentizar el rendimiento de algunas funcionalidades en XProtect Smart Client. Por ejemplo, XProtect Smart Client requiere un fotograma clave para empezar a mostrar vídeo, de modo que un periodo de tiempo más prolongado entre fotogramas clave prolonga el inicio de XProtect Smart Client.

Añadiendo hardware

Para obtener más información sobre cómo añadir hardware a su sistema, consulte Añadir hardware en la página 217.

Habilitar y deshabilitar la compatibilidad con lentes de ojo de pez

La compatibilidad con la lente ojo de pez está desactivada por defecto.

1. En el panel **Navegación del sitio**, seleccione **Dispositivos** y a continuación seleccione **Cámaras**.
2. Seleccione la cámara PTZ correspondiente en el panel **Generalidades**.
3. En la pestaña **Lente de ojo de pez**, seleccione o desactive la casilla **Habilitar soporte para ojo de pez**.

Especificar los ajustes de la lente ojo de pez

1. En la pestaña **Lente ojo de pez**, seleccione el tipo de lente.
2. Especifique la posición/orientación física de la cámara desde la lista **Posición/orientación de la cámara**.
3. Seleccione un número de lente panomórfica registrada (RPL) de la lista de **números RPL panomórficos de ImmerVision Enables®**.

   Esto garantiza la identificación y la configuración correcta del objetivo utilizado con la cámara. El número RPL suele hallarse en la propia lente o en la caja en la que viene. Para más información sobre ImmerVision, las lentes panomorfas y las RPL, consulte el sitio web de Immervision (https://www.immervisionenables.com/).

   Si selecciona el perfil de lente **Corrección de la distorsión esférica genérica** recuerde configurar el **Campo de visión** deseado.

Dispositivos - Grabación

Habilitar/deshabilitar la grabación

La grabación está habilitada por defecto. Para habilitar/deshabilitar la grabación:

1. En el panel **Navegación del sitio**, seleccione **Servidores de grabación**.
2. Seleccione el dispositivo correspondiente en el panel **Generalidades**.
3. En la pestaña **Grabar**, active o desactive la casilla **Grabación**.

Debe habilitar la grabación para el dispositivo antes de poder grabar datos de la cámara. Una regla que especifica las circunstancias para que un dispositivo grabe no funciona si ha desactivado la grabación para el dispositivo.

Habilitar la grabación en los dispositivos relacionados

En el caso de los dispositivos con cámara, puede habilitar la grabación para los dispositivos relacionados, por ejemplo, los micrófonos que estén conectados al mismo servidor de grabación. Significa que los dispositivos relacionados graban cuando la cámara graba.

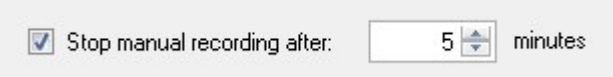
La grabación en dispositivos relacionados está habilitada por defecto para los nuevos dispositivos con cámara, pero puede deshabilitarla y habilitarla como desee. Para los dispositivos de cámara existentes en el sistema, la casilla está desactivada por defecto.

1. En el panel **Navegación del sitio**, seleccione **Servidores de grabación**.
2. Seleccione el dispositivo de cámara correspondiente en el panel **Generalidades**.
3. En la pestaña **Grabar**, seleccione o desactive la casilla **Grabar en dispositivos relacionados**.
4. En la pestaña **Cliente**, especifique los dispositivos relacionados con esta cámara.

Si desea habilitar la grabación en dispositivos relacionados que estén conectados a otro servidor de grabación, debe crear una regla.

Gestionar la grabación manual

Detener la grabación manual después está habilitado por defecto con un tiempo de grabación de cinco minutos. Esto es para asegurar que el sistema detenga automáticamente todas las grabaciones iniciadas por los usuarios de XProtect Smart Client.



1. En el panel **Navegación del sitio**, seleccione **Dispositivos**.
2. Seleccione el dispositivo correspondiente en el panel **Generalidades**.
3. En la pestaña **Grabar**, seleccione o desactive la casilla **Detener la grabación manual tras**.

Cuando lo habilite, especifique un tiempo de grabación. El número de minutos que especifique debe ser lo suficientemente grande como para acomodar los requisitos de las distintas grabaciones manuales sin sobrecargar el sistema.

Añadir a cometidos:

Debe conceder el permiso para iniciar y detener la grabación manual a los usuarios clientes en cada cámara en **Cometidos** en la pestaña **Dispositivo**.

Uso en reglas:

Los eventos que puede utilizar al crear reglas relacionadas con la grabación manual son:

- Grabación manual iniciada
- Grabación manual detenida

Especificar velocidad de grabación de fotogramas

Puede especificar la velocidad de grabación de fotogramas para JPEG.

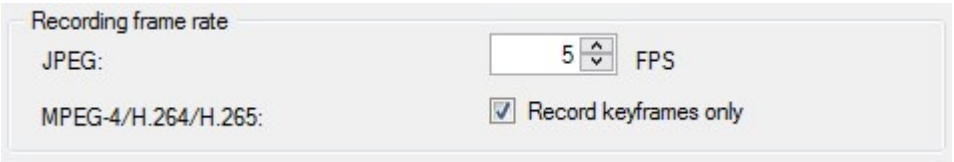
1. En el panel **Navegación del sitio**, seleccione **Dispositivos**.
2. Seleccione el dispositivo correspondiente en el panel **Generalidades**.
3. En la pestaña **Grabar**, en la **Velocidad de grabación de fotogramas: cuadro (JPEG)**, seleccione o introduzca la velocidad de grabación de fotogramas (en FPS, fotogramas por segundo).

Habilitar la grabación de fotogramas clave

Puede habilitar la grabación de fotogramas clave para flujos MPEG-4/H.264/H.265. Significa que el sistema cambia entre la grabación de fotogramas clave solo y la grabación de todos los fotogramas en función de la configuración de las reglas.

Puede, por ejemplo, dejar que el sistema grabe fotogramas clave cuando no hay movimiento en la vista y cambiar a todos los fotogramas solo en caso de detección de movimiento para ahorrar almacenamiento.

1. En el panel **Navegación del sitio**, seleccione **Dispositivos**.
2. Seleccione el dispositivo correspondiente en el panel **Generalidades**.
3. En la pestaña **Grabar**, active o desactive la casilla **Grabar solo fotogramas clave**.



4. Establezca una regla que active la función, consulte Acciones y acciones de detención.

Habilitar la grabación en los dispositivos relacionados

En el caso de los dispositivos con cámara, puede habilitar la grabación para los dispositivos relacionados, por ejemplo, los micrófonos que estén conectados al mismo servidor de grabación. Significa que los dispositivos relacionados graban cuando la cámara graba.

La grabación en dispositivos relacionados está habilitada por defecto para los nuevos dispositivos con cámara, pero puede deshabilitarla y habilitarla como desee. Para los dispositivos de cámara existentes en el sistema, la casilla está desactivada por defecto.

1. En el panel **Navegación del sitio**, seleccione **Servidores de grabación**.
2. Seleccione el dispositivo de cámara correspondiente en el panel **Generalidades**.
3. En la pestaña **Grabar**, seleccione o desactive la casilla **Grabar en dispositivos relacionados**.
4. En la pestaña **Cliente**, especifique los dispositivos relacionados con esta cámara.

Si desea habilitar la grabación en dispositivos relacionados que estén conectados a otro servidor de grabación, debe crear una regla.

Guardar y recuperar grabación remota

Para garantizar que todas las grabaciones remotas se guardan en caso de problemas de red, puede habilitar la recuperación automática de grabaciones una vez restablecida la conexión.

1. En el panel **Navegación del sitio**, seleccione **Dispositivos**.
2. Seleccione el dispositivo correspondiente en el panel **Generalidades**.
3. En **Grabaciones remotas**, seleccione **Recuperar automáticamente grabaciones remotas cuando se restaure la conexión**. Esto habilita la recuperación automática de grabaciones una vez restablecida la conexión

La opción de grabación remota solo está disponible si la cámara seleccionada es compatible con el almacenamiento periférico o es una cámara en una configuración de Milestone Interconnect.

El tipo de hardware seleccionado determina de dónde se recuperan las grabaciones:

- Para una cámara con almacenamiento de grabaciones local, las grabaciones se recuperan del almacenamiento de grabación local de la cámara
- Para un sistema remoto de Milestone Interconnect, las grabaciones se recuperan de los servidores de grabación del sistema remoto

Puede utilizar la siguiente funcionalidad independientemente de la recuperación automática:

- Grabación manual
- La regla **Recuperar y almacenar grabaciones remotas desde <dispositivos>**
- La regla **Recuperar y almacenar grabaciones remotas entre <hora de inicio y fin> desde <dispositivos>**

Borrar grabaciones

1. En el panel **Navegación del sitio**, seleccione **Dispositivos**.
2. Seleccione el dispositivo correspondiente en el panel **Generalidades** y seleccione la pestaña **Grabación**.
3. Haga clic en el **Eliminar todas las grabaciones** para eliminar todas las grabaciones del dispositivo o grupo de dispositivos.

Este método solo puede utilizarse si ha añadido todos los dispositivos del grupo al mismo servidor. Los datos protegidos no están eliminados.

Dispositivos - Ajustes de cámara

Transmisión adaptable (explicación)

El streaming adaptativo es un método de transmisión que se utiliza al exhibirse varios flujos de vídeo en directo en la misma vista. Permite a los clientes seleccionar automáticamente las transmisiones de vídeo en directo cuya resolución coincide mejor con las transmisiones solicitadas por los elementos de vista. El streaming adaptativo reduce la carga de la red y mejora la capacidad de descodificación y el rendimiento del ordenador del cliente.

Puede configurar la coincidencia más cercana de transmisiones de vídeo disponibles para la resolución solicitada por un elemento de vista al habilitar un streaming adaptativo en XProtect Smart Client. Para obtener más información, consulte Habilitar el streaming adaptativo.

En XProtect Smart Client, el streaming adaptativo puede aplicarse en modo directo y modo reproducción. En los clientes móviles, únicamente está disponible en modo directo.

Al aplicarse en modo reproducción, el método de streaming se denomina reproducción adaptativa. Si desea más información, consulte Reproducción adaptativa (explicado) en la página 237

Reproducción adaptativa (explicado)

La reproducción adaptativa es una configuración que permite el uso de streaming adaptativo en modo reproducción.

La reproducción adaptativa requiere dos transmisiones de grabación, una primaria y otra secundaria. Si ambas transmisiones están habilitadas en el Management Client, ambas estarán grabando.

- Si se reproduce vídeo de un periodo anterior a la configuración de la grabación secundaria, solamente se reproducirán las grabaciones primarias.
- Si se reproduce vídeo grabado después de configurar la grabación secundaria, el vídeo se reproducirá a partir de la grabación primaria o de la secundaria, en función de la que mejor se adapte al tamaño de visualización del cliente.

Disponibilidad

> La funcionalidad disponible depende del sistema que esté utilizando. Vea la lista completa de características, que está disponible en la página de descripción del producto en el sitio web Milestone (https://www.milestonesys.com/solutions/platform/product-index/).

Activar streaming adaptable

Puede activar la reproducción adaptativa junto con el streaming adaptativo en la pestaña **Avanzado** en **Perfiles de cliente inteligente** y también debe estar habilitado en XProtect Smart Client en la ventana **Configuraciones** > **Avanzado** > **Streaming adaptativo**. Para obtener más información sobre cómo habilitar streaming adaptativo en XProtect Smart Client, consulte Habilitar transmisión adaptable

Grabaciones en Edge

Opcionalmente, se pueden utilizar grabaciones de Edge para la reproducción adaptativa. Las grabaciones de Edge permiten ver secuencias de una transmisión con una resolución diferente, normalmente superior a la del resto de la transmisión. Por ejemplo, puede grabar una transmisión primaria con una resolución baja y fusionar grabaciones de una fuente de alta resolución. Puede activar las grabaciones de Edge fusionadas cuando navegue por los datos.

Las grabaciones de Edge se almacenan en la base de datos de medios y la resolución de estas grabaciones se establece en cámaras individuales.

Resolución del vídeo reproducido

Al utilizarse la reproducción adaptativa, la resolución del vídeo reproducido viene determinada por los ajustes de resolución actuales de las grabaciones primaria y secundaria. Es decir, en la reproducción, la elección del flujo primario o secundario se basa en la resolución configurada actualmente para las respectivas transmisiones de grabación.

Añadir un flujo

Las transmisiones que añada para grabar se pueden ver en directo y en modo reproducción.

También puede ver el vídeo grabado en su elemento de vista con la transmisión habilitada. El streaming adaptativo en modo reproducción se denomina reproducción adaptativa.

1. En la pestaña **Flujos**, haga clic en **Añadir**. Esto añade un segundo flujo a la lista.
2. En la columna **Nombre**, edite el nombre del flujo. El nombre aparece en XProtect Smart Client.
3. En la columna **Modo en directo**, seleccione cuándo se necesita la transmisión en directo:
    - **Siempre**: el flujo se ejecuta incluso si ningún usuario de XProtect Smart Client lo solicita
    - **Nunca**: la transmisión está desconectada. Utilícelo solo para grabar flujos, por ejemplo, si quiere grabar en alta calidad y necesita el ancho de banda
    - **Cuando sea necesario**: la transmisión se inicia cuando lo solicita cualquier cliente o si el flujo está configurado para grabar
4. En la columna **Transmisión en directo por defecto**, seleccione qué transmisión es el predeterminado y debe utilizarse si el cliente no solicita una transmisión específica y el streaming adaptativo está desactivado.

5. En la columna **Grabación**, seleccionar **Primario** o **Secundario**. Para la reproducción adaptativa, deberá crear una transmisión de cada tipo. El vídeo que se reproduce procede de la transmisión de vídeo primaria y se incluye un flujo secundario cuando es necesario. Siempre tiene que haber una grabación primaria. Además, la transmisión que configure como **Primario** se utilizará en diferentes contextos, como para la detección de movimiento y para la exportación desde XProtect Smart Client.
6. En **Reproducción por defecto**, seleccione qué transmisión es la predeterminada. La transmisión predeterminada se entregará al cliente si la reproducción adaptativa no está configurada.
7. En la columna **Utilizar grabaciones de Edge**, seleccione la casilla si desea utilizar grabaciones de Edge. Para obtener más información sobre las grabaciones de Edge, consulte Grabaciones en Edge en la página 238.
8. Haga clic en **Guardar**.

Si no quiere que las transmisiones se ejecuten en absoluto a menos que alguien esté viendo vídeo en directo, puede modificar la **Regla de inicio de transmisión por defecto** para que se inicie a petición con el evento predefinido **Entrada de cliente en directo solicitada**.

Gestionar la transmisión múltiple

La visualización de vídeo en directo y la reproducción de vídeo grabado no requieren necesariamente la misma calidad de vídeo y velocidad de fotogramas.

Para cambiar el flujo que se utilizará para la grabación

La reproducción adaptativa requiere que dos transmisiones estén configuradas para grabar, una primaria y otra secundaria. Para la transmisión en directo, puede configurar y utilizar tantas transmisiones en directo como admita la cámara.

1. En el panel **Navegación del sitio**, seleccione **Dispositivos**.
2. Seleccione la cámara correspondiente en el panel **Generalidades**.
3. En la pestaña **Transmisiones**, seleccione la transmisión que desee para la grabación.
4. Seleccione la opción pertinente en la lista **Modo directo**. Las opciones **Cuando sea necesario**, **Siempre** y **Nunca** indican cuándo debería aplicarse la transmisión en el cliente. Si no se solicita nada al cliente, la grabación utilizará la transmisión en la que esté activada la casilla **Transmisión en directo por defecto**.
5. Para grabar en una transmisión, seleccione **Primario** o **Secundario** en la lista de **Grabaciones**.
6. Para utilizar la reproducción adaptativa, configure dos transmisiones y ajuste una de ellas a **Primario** y la otra a **Secundario**.
7. Para grabar en una transmisión, seleccione **Primario** o **Secundario** en la lista de **Grabaciones**.

Limitar la transmisión de datos

Puede configurar un conjunto de condiciones para garantizar que los flujos de vídeo solo se ejecuten cuando los vea un cliente.

Para gestionar la transmisión de datos y limitar las transmisiones innecesarias, la transmisión no se inicia cuando se cumplen las siguientes condiciones:

1. En el panel **Navegación del sitio**, seleccione **Dispositivos**.
2. Seleccione la cámara correspondiente en el panel **Generalidades**.
3. En la pestaña **Flujos**, en la lista **Modo en directo**, seleccione **Cuando sea necesario**.
4. En la pestaña **Grabar**, desactive la casilla **Grabación**.
5. En la pestaña **Movimiento**,desmarque la casilla **Detección de movimiento**.

Si se cumplen estas condiciones, los flujos de vídeo solo se ejecutarán cuando los vea un cliente.

Ejemplos

Ejemplo 1, vídeo en directo y grabado:

- Para la visualización de vídeo **en directo**, su organización puede preferir H.264 con una alta velocidad de fotogramas
- Para reproducir el vídeo **grabado**, su organización puede preferir MJPEG a una velocidad de fotogramas inferior para preservar el espacio en disco

Ejemplo 2, vídeo en directo local y remoto:

- Para la visualización de **vídeo en directo desde un punto operativo conectado localmente**, su organización puede preferir H.264 con una alta tasa de fotogramas para tener la máxima calidad de vídeo disponible
- Para la visualización de **vídeo en directo desde un punto de operación conectado de forma remota**, su organización puede preferir MJPEG a una velocidad de fotogramas y calidad inferiores para preservar el ancho de banda de la red

Ejemplo 3, streaming adaptable:

- Para la visualización de **vídeo en directo y la disminución de la carga de la CPU y la GPU del ordenador XProtect Smart Client**, su organización puede preferir múltiples H.264/H.265 de alta velocidad de fotogramas, pero con diferentes resoluciones para adaptarse a la resolución solicitada por XProtect Smart Client cuando se utiliza el streaming adaptable. Si desea más información, consulte Smart Client Perfiles (nodo Cliente) en la página 488.

Si habilita la **Multidifusión en directo** en la pestaña **Cliente** de la cámara (consulte la pestaña Cliente (dispositivos)), solo funciona en el flujo de vídeo predeterminado.

Incluso cuando las cámaras admiten la transmisión múltiple, las capacidades individuales de transmisión múltiple pueden variar entre las distintas cámaras. Consulte la documentación de la cámara para obtener más información.

Para ver si una cámara ofrece diferentes tipos de secuencias, consulte la pestaña **Configuración (dispositivos)**.

Dispositivos - Almacenamiento

Gestionar almacenamiento previo en búfer

Las cámaras, los micrófonos y los altavoces admiten el almacenamiento previo en búfer. En el caso de los altavoces, los flujos sólo se envían cuando el usuario de XProtect Smart Client utiliza la función **Hablar con el altavoz**. Esto es útil cuando se quiere grabar el audio o el vídeo que conduce a un evento que activa la grabación, por ejemplo, la apertura de una puerta.

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 estos casos, no hay disponible ningún pre-buffer de altavoz.

Para utilizar la función de pre-buffer, los dispositivos deben estar habilitados y enviar un flujo al sistema.

Habilitar y deshabilitar almacenamiento previo en búfer

El almacenamiento previo en búfer está habilitado por defecto con un tamaño de pre-buffer de tres segundos y almacenamiento en la memoria.

1. En el panel **Navegación del sitio**, seleccione **Dispositivos**.
2. Seleccione el dispositivo correspondiente en el panel **Generalidades**.
3. En la pestaña **Grabar**, seleccione o desactive la casilla **Grabación**.
4. En la pestaña **Cliente**, especifique los dispositivos relacionados con esta cámara.

Especificar el lugar de almacenamiento y el periodo de pre-búfer

Las grabaciones temporales del pre-buffer se almacenan en la memoria o en el disco:

1. En el panel **Navegación del sitio**, seleccione **Dispositivos**.
2. Seleccione el dispositivo correspondiente en el panel **Generalidades** y seleccione la pestaña **Grabar**.
3. En la lista **Ubicación**, seleccione **Memoria** o **Disco**, y especifique el número de segundos.
4. Si necesita un periodo de pre-buffer de más de 15 segundos, seleccione **Disco**.

El número de segundos que especifique debe ser lo suficientemente grande como para adaptarse a sus necesidades en las distintas reglas de grabación que defina.

Si cambia la ubicación a **Memoria**, el sistema redujo el periodo a 15 segundos automáticamente.

Usar el pre-buffer en las reglas

Cuando creas reglas que activan la grabación, puedes seleccionar que las grabaciones comiencen algún tiempo antes del evento real (pre-buffer).

Ejemplo: La siguiente regla especifica que la grabación debe comenzar en la cámara 5 segundos antes de que se detecte movimiento en la cámara.

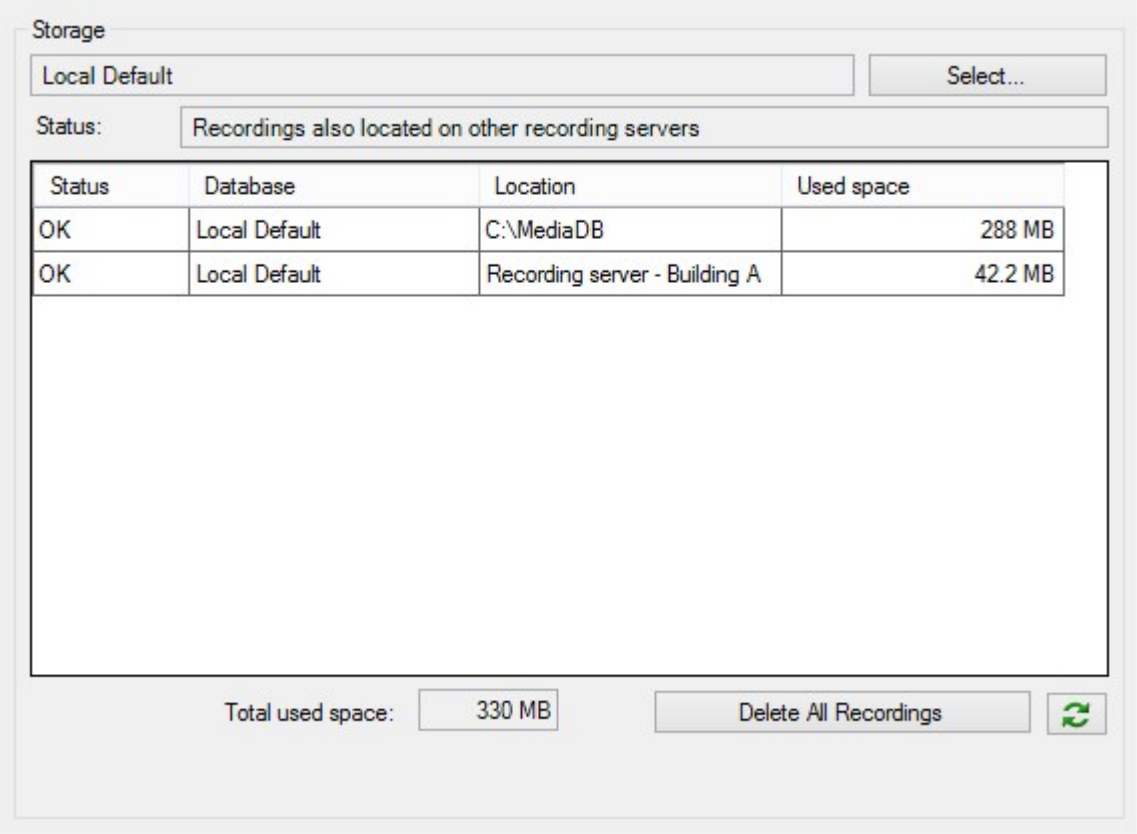
Para utilizar la función de grabación de prebuffer en la regla, debe habilitar el almacenamiento previo en búfer en el dispositivo que se está grabando y debe ajustar la longitud del pre-buffer al menos a la misma longitud especificada en la regla.

Monitorizar el estado de las bases de datos para dispositivos

1. En el panel **Navegación del sitio**, seleccione **Dispositivos**.
2. Seleccione el dispositivo correspondiente en el panel **Generalidades** y seleccione la pestaña **Grabación**.

En **Almacenamiento**, puede supervisar y gestionar las bases de datos de un dispositivo o de un grupo de dispositivos añadidos al mismo servidor de grabación.

Encima de la tabla, puede ver la base de datos seleccionada y su estado. En este ejemplo, la base de datos seleccionada es la **Local por defecto** por defecto y el estado es **Grabaciones ubicadas también en otros servidores de grabación**. El otro servidor es el de grabación del edificio A.



Posibles estados 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 ubicadas en almacenes de otros servidores de grabación también.
Los archivos también se encuentran en el almacenamiento anterior	La base de datos está activa y funcionando y tiene archivos ubicados en otros almacenamientos también.
Activo	La base de datos está activa y funcionando.
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 está moviendo los datos de uno o varios dispositivos seleccionados de un grupo de una ubicación a otra.

Nombre	Descripción
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 está moviendo los datos del 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 ésta se encuentra en modo failover.

Más abajo en la ventana, puede ver el estado de cada base de datos (**Aceptar**, **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, puede ver el espacio total utilizado para todo el almacenamiento en el campo **Espacio total utilizado**.

Para obtener información sobre la configuración del almacenamiento, consulte la pestaña Almacenamiento (servidor de grabación).

Mover dispositivos de un almacenamiento a otro

> Cuando seleccione una nueva ubicación para almacenar las grabaciones, las grabaciones existentes no se moverán. Permanecerán en la ubicación actual, con las condiciones definidas por la configuración del almacenamiento al que pertenecen.

1. En el panel **Navegación del sitio**, seleccione **Dispositivos**.
2. Seleccione el dispositivo correspondiente en el panel **Generalidades** y seleccione la pestaña **Grabación**.
3. Haga clic en **Seleccionar** en **Almacenamiento** para seleccionar un almacenamiento de grabación para que sus dispositivos graben.

Las grabaciones se archivarán según la configuración del almacenamiento que seleccione.

Dispositivos - Detección de movimiento

Detección de movimiento (explicación)

La configuración de la detección de movimiento es un elemento clave en su sistema: Su configuración de detección de movimiento determina cuándo el sistema genera eventos de movimiento y normalmente también cuándo se graba el vídeo.

El tiempo dedicado a encontrar la mejor configuración de detección de movimiento posible para cada cámara le ayudará a evitar posteriormente, por ejemplo, grabaciones innecesarias. Dependiendo de la ubicación física de la cámara, puede ser una buena idea probar los ajustes de detección de movimiento en diferentes condiciones físicas, como el día/la noche y el tiempo ventoso/calmado.

Puede especificar los ajustes relacionados con la cantidad de cambios necesarios en la vista de una cámara para que el cambio se considere movimiento. Puede, por ejemplo, especificar los intervalos entre el análisis de detección de movimiento y las áreas de una vista en las que el movimiento debe ser ignorado. También puede ajustar la precisión de la detección de movimiento y, por tanto, la carga de los recursos del sistema.

Calidad de imagen

Antes de configurar la detección de movimiento para una cámara, Milestone recomienda haber configurado los ajustes de calidad de imagen de la cámara, por ejemplo, la resolución, el códec de vídeo y los ajustes de flujo. Esto se hace en la pestaña **Ajustes** de la ventana **Propiedades** del dispositivo. Si posteriormente cambia la configuración de la calidad de la imagen, siempre debe probar después cualquier configuración de detección de movimiento.

Máscaras de privacidad

Si ha definido áreas con máscaras de privacidad permanentes, no hay detección de movimiento dentro de estas áreas.

Habilitar y deshabilitar la detección de movimiento

Especificar la configuración por defecto de detección de movimiento para cámaras

1. En el menú **Herramientas**, haga clic en **Opciones**.
2. En la pestaña **General**, en **Al añadir nuevos dispositivos de cámara habilitar automáticamente**, seleccione la casilla **Detección de movimiento**.

Habilitar o deshabilitar la detección de movimiento para una cámara específica

1. En el panel **Navegación del sitio**, seleccione **Dispositivos** y a continuación seleccione **Cámaras**.
2. Seleccione la cámara correspondiente en el panel **Generalidades**.
3. En la **pestaña Movimiento**, active o desmarque la casilla **Detección de movimiento**.

Cuando deshabilita la detección de movimiento para una cámara, las reglas relacionadas con la detección de movimiento para la cámara no funcionan.

Habilitar o deshabilitar la aceleración por hardware

La decodificación automática de vídeo acelerada por hardware para la detección de movimiento es la configuración por defecto cuando se añade una cámara. El servidor de grabación utiliza los recursos de la GPU si están disponibles. Esto reducirá la carga de la CPU durante el análisis del movimiento del vídeo y mejorará el rendimiento general del servidor de grabación.

Para habilitar o deshabilitar la aceleración por hardware

1. En el panel **Navegación del sitio**, seleccione **Dispositivos**.
2. Seleccione la cámara correspondiente en el panel **Generalidades**.
3. En la pestaña **Movimiento**, en **Aceleración por hardware** seleccione **Automático** para habilitar la aceleración por hardware o seleccione **Desactivado** para desactivar la configuración.

Uso de recursos de la GPU

La decodificación de vídeo acelerada por hardware para la detección de movimiento utiliza recursos de la GPU en:

- Las CPU Intel que admiten Intel Quick Sync
- NVIDIA® muestra adaptadores de pantalla conectados a su servidor de grabación

Equilibrio de carga y rendimiento

El equilibrio de la carga entre los diferentes recursos se realiza automáticamente. En el nodo **Monitor del sistema** puede verificar si la carga actual de análisis de movimiento 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

Si la carga es demasiado alta, puede añadir recursos de GPU a su servidor de grabación instalando varios adaptadores de pantalla NVIDIA. Milestone desaconseja el uso de la configuración SLI (Scalable Link Interface) de tarjetas gráficas NVIDIA.

Los productos NVIDIA tienen diferentes capacidades de computación.

La decodificación de vídeo acelerada por hardware para la detección de movimiento utilizando las GPU NVIDIA requiere una capacidad de cálculo de la versión 6.x (Pascal) o más reciente.

- Para buscar la versión de capacidad de computación de su producto NVIDIA, visite el sitio web de NVIDIA (https://developer.nvidia.com/cuda-gpus/).
- Para ver si la detección de movimiento de vídeo está acelerada por hardware para una cámara específica, habilite el registro en el archivo de registro del servidor de grabación. Establezca el nivel en **Depuración** y el diagnóstico se registrará en el DeviceHandling.log. El registro sigue el patrón: [time] [274] DEBUG – [guid] [name] Descodificación configurada: Automática: Decodificación real: Intel/NVIDIA

La versión del sistema operativo del servidor de grabación y la generación de la CPU pueden afectar al rendimiento de la detección de movimiento de vídeo acelerada por hardware. La asignación de memoria a la GPU suele ser el cuello de botella con las versiones más antiguas (el límite típico está 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 la GPU y así eliminar o reducir este cuello de botella.

La 6ª generación de las CPU de Intel sí proporciona decodificación acelerada por hardware de H.265, por lo que el rendimiento es comparable al de H.264 para estas versiones de CPU.

Habilitar la sensibilidad manual para definir el movimiento

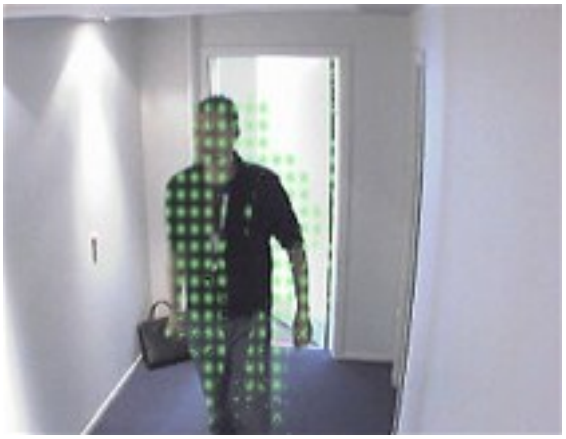
El ajuste de la sensibilidad determina **cuánto debe cambiar cada píxel** de la imagen para que se considere movimiento.

1. En el panel **Navegación del sitio**, seleccione **Dispositivos** y a continuación seleccione **Cámaras**.
2. Seleccione la cámara correspondiente en el panel **Generalidades**.
3. Seleccione la casilla **Sensibilidad manual** de la pestaña **Movimiento**.
4. Arrastre el control deslizante hacia la izquierda para un nivel de sensibilidad más alto, y hacia la derecha para un nivel de sensibilidad más bajo.

   Cuanto **más alto** sea el nivel de sensibilidad, menos cambio se permite en cada píxel antes de considerarlo como movimiento.

   Cuanto **más bajo** sea el nivel de sensibilidad, mayor será el cambio permitido en cada píxel antes de considerarlo como movimiento.

   Los píxeles en los que se detecta movimiento se resaltan en verde en la imagen de vista previa.
5. Seleccione una posición del deslizador en la que solo se resalten las detecciones que considere de movimiento.



Puede comparar y establecer el ajuste exacto de sensibilidad entre las cámaras mediante el número que aparece en la parte derecha del control deslizante.

Especificar umbral para definir movimiento

El umbral de detección de movimiento determina **la cantidad de píxeles** de la imagen deben cambiar antes de que se considere movimiento.

1. Arrastre el control deslizante a la izquierda para un mayor nivel de movimiento y a la derecha para un menor nivel de movimiento.
2. Seleccione una posición del control deslizante en la que solo se detecten las detecciones que usted considera movimiento.

La línea negra vertical en la barra de indicación de movimiento muestra el umbral de detección de movimiento: Cuando el movimiento detectado está por encima del nivel del umbral de detección seleccionado, la barra cambia de color de verde a rojo, lo que indica una detección positiva.

Barra de indicación de movimiento: cambia de color, de verde a rojo, cuando está por encima del umbral, lo que indica una detección positiva de movimiento.

Especificar regiones de exclusión para detección de movimiento

Puede configurar todos los ajustes para un grupo de cámaras, pero normalmente establecería las regiones de exclusión por cámara.

Las áreas con máscaras de privacidad permanente también quedan excluidas de la detección de movimiento. Seleccione la casilla de verificación **Mostrar máscaras de privacidad** para mostrarlas.

Excluir la detección de movimiento de un área concreta le ayuda a evitar la detección de movimiento irrelevante, por ejemplo, si la cámara cubre un área en la que un árbol se está balanceando por el viento o cuando pasan coches regularmente en segundo plano.

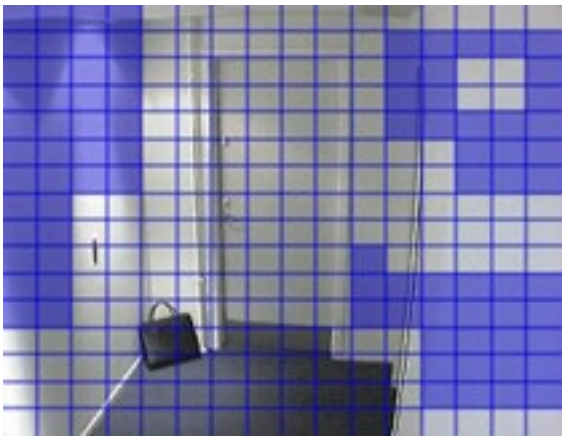
Al utilizar regiones de exclusión con cámaras PTZ y utilizar panorámica-inclinación-zoom en la cámara, el área excluida **no** se mueve en consonancia, porque el área está bloqueada para la imagen de la cámara, y no para el objetivo.

1. Para utilizar regiones de exclusión, seleccione la casilla de verificación **Usar regiones de exclusión**.

   Una cuadrícula divide la imagen de la vista previa en secciones seleccionables.

2. Para definir regiones de exclusión, arrastre el puntero del ratón por las áreas requeridas en la imagen de vista previa mientras pulsa el botón izquierdo del ratón. El botón derecho del ratón borra una sección de la cuadrícula.

Puede definir tantas regiones de exclusión como sea necesario. Las regiones excluidas aparecen en azul:



Las áreas azules excluidas aparecen en la imagen de vista previa en la pestaña **Movimiento**, no en ninguna otra imagen de vista previa en Management Client o en clientes de acceso.

Dispositivos - Posiciones de cámara preestablecidas

La posición prestablecida inicial

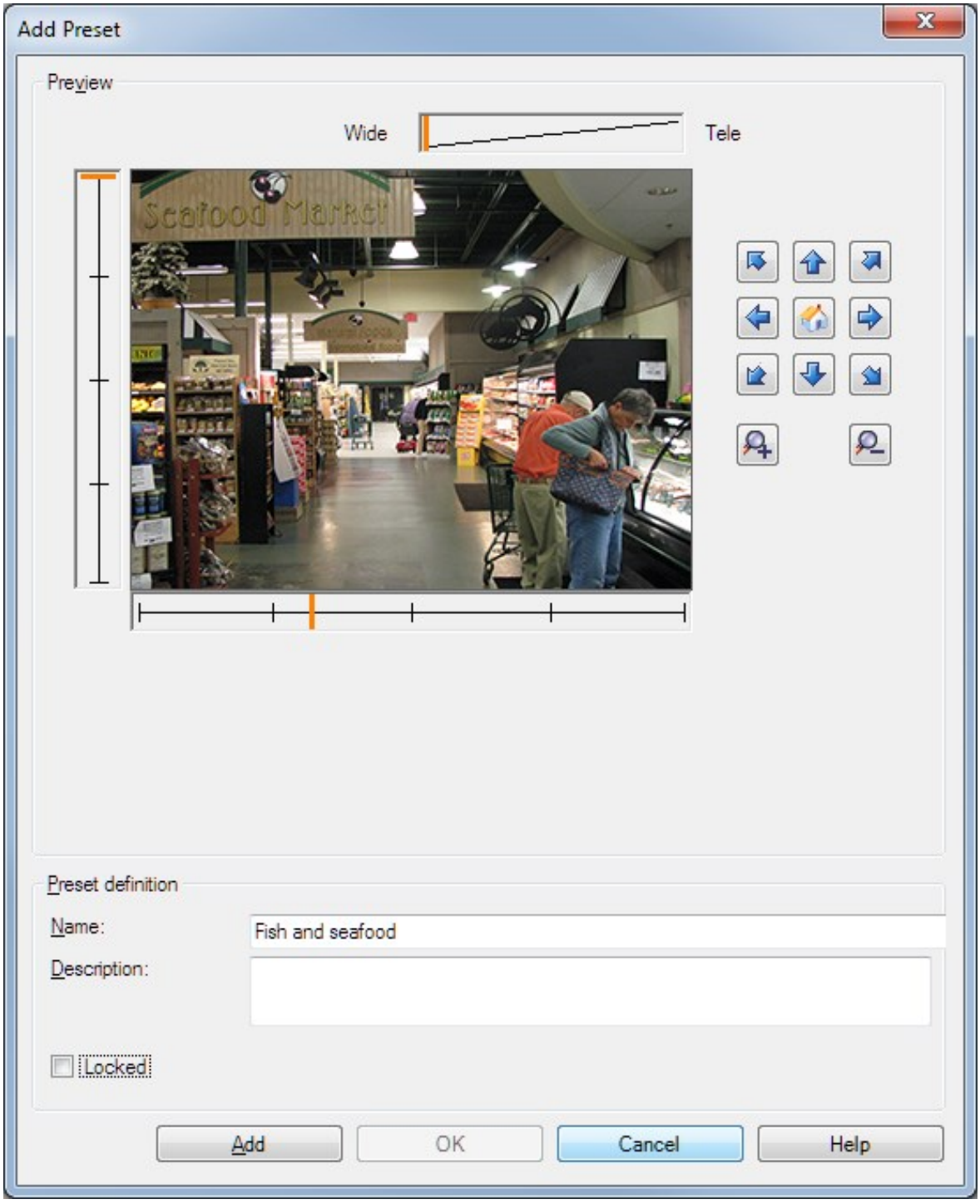
La posición prestablecida de la cámara se define en la página de inicio de la cámara. Las capacidades PTZ disponibles en la página de inicio dependen de la cámara.

Añadir una posición preestablecida (tipo 1)

Para añadir una posición preestablecida para la cámara:

1. En el panel **Navegación del sitio**, seleccione **Dispositivos** y a continuación seleccione **Cámaras**.
2. Seleccione la cámara PTZ correspondiente en el panel **Generalidades**.

3. En la pestaña **Valores preestablecidos**, haga clic en **Nuevo**. Aparece la ventana **Añadir valor preestablecido**:



4. La ventana **Añadir valor preestablecido** muestra una imagen de vista previa en directo de la cámara. Utilice los botones de navegación y/o los controles deslizantes para mover la cámara a la posición deseada.
5. Especifique un nombre para la posición preestablecida en el campo **Nombre**.
6. Opcionalmente, introduzca una descripción de la posición preestablecida en el campo **Descripción**.
7. Seleccione **Bloqueado** si desea bloquear la posición preestablecida. Solo los usuarios con permisos suficientes pueden desbloquear la posición después.
8. Haga clic en **Añadir** para especificar valores preestablecidos. Siga añadiendo hasta tener los valores preestablecidos que desee.
9. Haga clic en **Aceptar**. La ventana **Añadir valor preestablecido** se cierra y añade la posición a la lista de la pestaña **Valores preestablecidos** de las posiciones preestablecidas disponibles para la cámara.

Utilizar posiciones predefinidas desde la cámara (tipo 2)

Como alternativa a especificar posiciones predefinidas en el sistema, puede especificar posiciones predefinidas para algunas cámaras PTZ en la propia cámara. Normalmente puede hacerlo accediendo a la página web de configuración específica de un producto.

1. En el panel **Navegación del sitio**, seleccione **Dispositivos** y a continuación seleccione **Cámaras**.
2. Seleccione la cámara PTZ correspondiente en el panel **Generalidades**.
3. En la pestaña **Valores preestablecidos**, seleccione **Utilizar valores preestablecidos del dispositivo** para importar los valores preestablecidos en el sistema.

   Cualquier ajuste predefinido que haya definido previamente para la cámara se elimina y afecta a cualquier regla definida y a los calendarios de vigilancia, además de eliminar los valores preestablecidos predefinidos disponibles para los usuarios de XProtect Smart Client s.
4. Haga clic en **Eliminar** para eliminar valores preestablecidos que sus usuarios no necesitan.
5. Haga clic en **Editar** si quiere cambiar el nombre de la visualización del ajuste predefinido (consulte Cambiar nombre de una posición predefinida (solo tipo 2)).
6. Si más adelante quiere editar dichos valores preestablecidos definidos por el usuario, edite en la cámara y luego vuelta a importar.

Asignar la posición prestablecida de una cámara como predeterminada

Si lo desea, puede asignar una de las posiciones preestablecidas de una cámara PTZ como la posición preestablecida por defecto de la cámara.

Puede ser útil tener una posición preestablecida por defecto porque le permite definir reglas que especifican que la cámara PTZ debe ir a la posición preestablecida por defecto en circunstancias particulares, por ejemplo después de haber operado la cámara PTZ manualmente.

1. En el panel **Navegación del sitio**, seleccione **Dispositivos** y a continuación seleccione **Cámaras**.
2. Seleccione la cámara PTZ correspondiente en el panel **Generalidades**.
3. En la pestaña **Valores preestablecidos**, en **Posiciones preestablecidas**, seleccione el valor preestablecido en su lista de posiciones preestablecidas definidas.
4. Seleccione la casilla **Valor preestablecido por defecto** debajo de la lista.

Solo puede definir una posición preestablecida como posición preestablecida por defecto.

Si ha seleccionado **Usar valor prestablecido como posición de inicio de PTZ** en **Opciones** > **General**, se utilizará la posición prestablecida de forma predeterminada en lugar de la posición de inicio definida de la cámara PTZ.

Especificar el valor prestablecido predeterminado como la posición de inicio de PTZ

Los usuarios de Management Client y XProtect Smart Client con los permisos de usuario necesarios pueden configurar el sistema para utilizar la posición prestablecida predeterminada en lugar de la posición de inicio de las cámaras PTZ si se activa el botón **Inicio** en un cliente.

Se debe definir una posición prestablecida para la cámara. Si no se define una posición prestablecida, no ocurrirá nada al activar el botón **Inicio** en un cliente.

Habilitar configuración de la posición de inicio de PTZ

1. Seleccione **Herramientas** > **Opciones**.

2. En la pestaña **General**, en el grupo **Servidor de grabación**, seleccione **Utilizar valor prestablecido predeterminado como posición de inicio de PTZ**.

3. Asigne una posición prestablecida como posición prestablecida predeterminada para la cámara.

Para asignar una posición prestablecida predeterminada, consulte Asignar la posición prestablecida de una cámara como predeterminada en la página 252

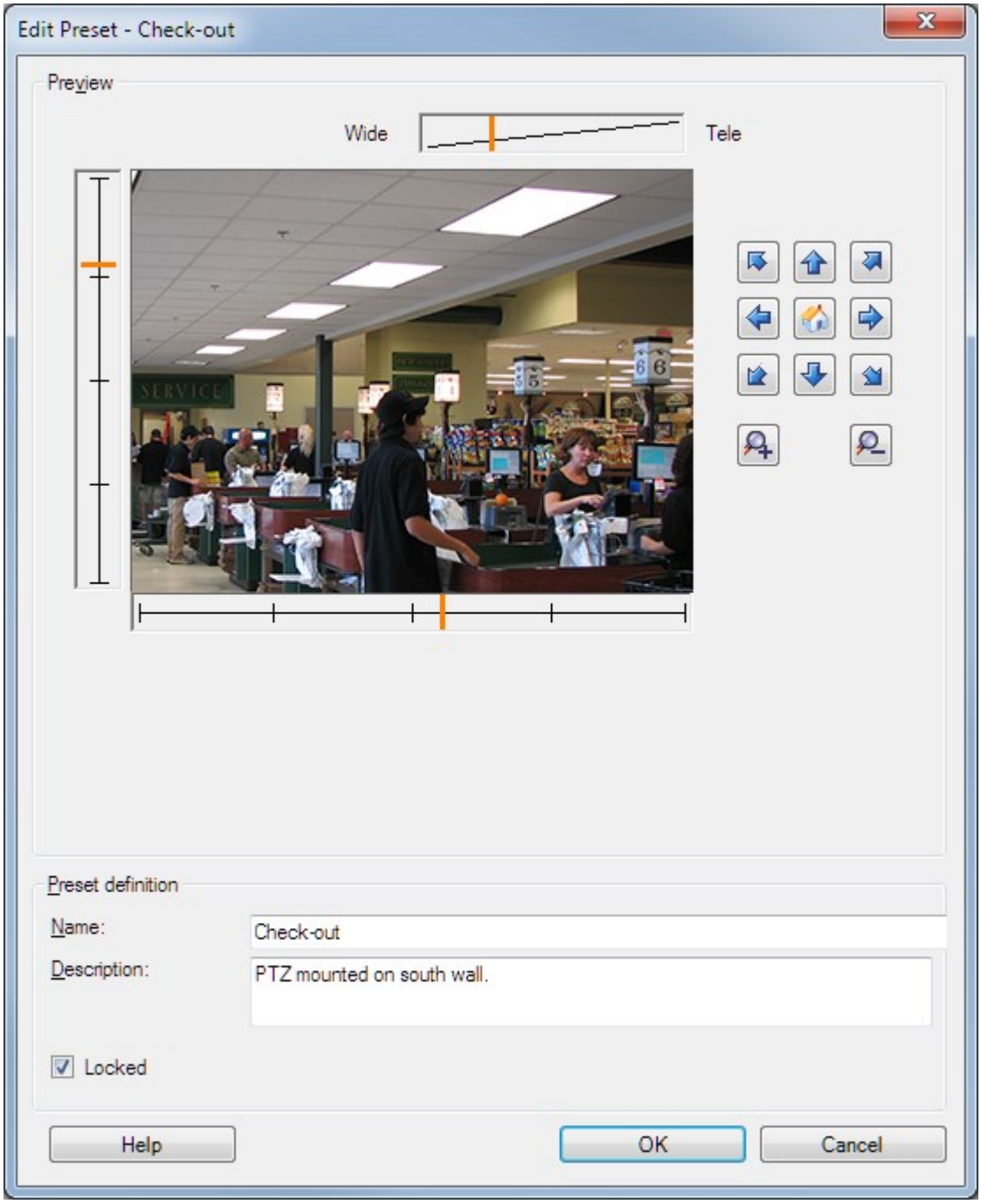
Consulte también Ajustes del sistema (cuadro de diálogo Opciones) en la página 396

Editar una posición preestablecida para una cámara (solo tipo 1)

Para editar una posición preestablecida existente definida en el sistema:

1. En el panel **Navegación del sitio**, seleccione **Dispositivos** y a continuación seleccione **Cámaras**.
2. Seleccione la cámara correspondiente en el panel **Generalidades**.
3. En la pestaña **Valores preestablecidos**, en Posiciones preestablecidas, seleccione la posición preestablecida en la lista de posiciones preestablecidas disponibles para la cámara.

4. Haga clic en **Editar**. Se abre la ventana **Editar valores preestablecidos**:



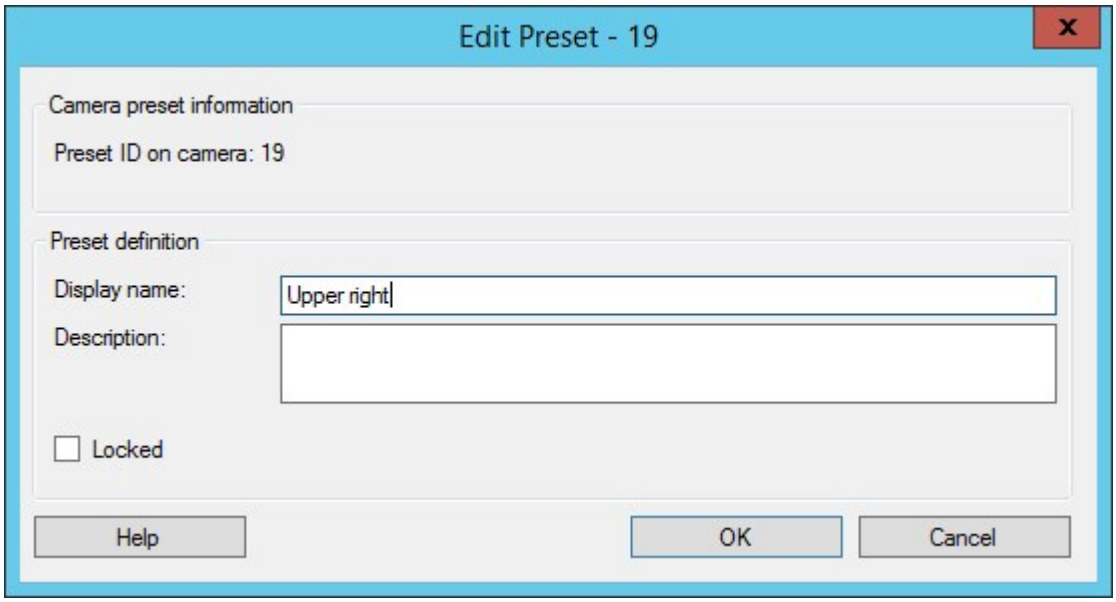
5. La ventana de **Editar valor preestablecido** muestra el vídeo en directo desde la posición preestablecida. Utilice los botones de navegación y/o los controles deslizantes para cambiar la posición preestablecida según sea necesario.
6. Cambie el nombre/número y la descripción de la posición preestablecida si es necesario.

7. Seleccione **Bloqueado** si desea bloquear la posición preestablecida. Solo los usuarios con permisos suficientes pueden desbloquear la posición después.
8. Haga clic en **Aceptar**.

Cambiar el nombre de una posición predefinida para una cámara (solo tipo 2)

Para editar el nombre de la posición predefinida definida en la cámara:

1. En el panel **Navegación del sitio**, seleccione **Dispositivos** y a continuación seleccione **Cámaras**.
2. Seleccione la cámara PTZ correspondiente en el panel **Generalidades**.
3. Seleccione la posición predefinida en la lista de valores preestablecidos disponibles de la pestaña **Valores preestablecidos** para la cámara.
4. Haga clic en **Editar**. Se abre la ventana **Editar valores preestablecidos**:



5. Cambie el nombre y añada una descripción de la posición predefinida, si fuera necesario.
6. Seleccione **Bloqueado** si quiere bloquear el nombre predefinido. Puede bloquear el nombre de un valor preestablecido si desea evitar que los usuarios de XProtect Smart Client o con permisos de seguridad limitados actualicen el nombre del valor preestablecido o lo eliminen. Los valores preestablecidos bloqueados se indican con este icono . Solo los usuarios con permisos suficientes pueden desbloquear el nombre preestablecido después.
7. Haga clic en **Aceptar**.

Probar una posición predefinida (solo tipo 1)

1. En el panel **Navegación del sitio**, seleccione **Dispositivos** y a continuación seleccione **Cámaras**.
2. Seleccione la cámara PTZ correspondiente en el panel **Generalidades**.
3. Seleccione la posición preestablecida en la lista de posiciones preestablecidas de la pestaña **Valores preestablecidos** para la cámara.
4. Haga clic en **Activar**.
5. La cámara se mueve a la posición predefinida seleccionada.

Dispositivos - Patrulla

Perfiles de patrulla y Patrulla manual (explicación)

Los perfiles de la patrulla son las definiciones de cómo debe tener lugar la patrulla. Esto incluye el orden en que la cámara debe moverse entre las posiciones preestablecidas y el tiempo que debe permanecer en cada posición. Puede crear un número ilimitado de perfiles de patrulla y utilizarlos en sus reglas. Por ejemplo, puede crear una regla que especifique que se debe utilizar un perfil de patrulla durante el horario diurno y otro durante el nocturno.

Patrulla manual

Antes de aplicar un perfil de patrulla en una regla, por ejemplo, puede probar el perfil de patrulla con un patrulla manual. También puede utilizar el patrullaje manual para hacerse cargo del patrullaje de otro usuario o de un patrullaje activado por reglas, siempre que tenga una prioridad PTZ más alta.

Si la cámara ya está patrullando o es controlada por otro usuario, solo podrá iniciar el patrullaje manual si tiene una prioridad mayor.

Si inicia una patrulla manual mientras la cámara ejecuta una patrulla de sistema activada por reglas, el sistema reanuda esta patrulla cuando detiene su patrulla manual. Si otro usuario ejecuta una patrulla manual, pero usted tiene una prioridad más alta y comienza su patrulla manual, la patrulla manual del otro usuario no se reanuda.

Si no detiene la patrulla manual por su cuenta, ésta continuará hasta que una patrulla basada en reglas o un usuario con mayor prioridad se haga cargo. Cuando la patrulla del sistema basado en reglas se detiene, el sistema reanuda su patrulla manual. Si otro usuario inicia una patrulla manual, su patrulla manual se detiene y no se reanudará.

Cuando se detiene la patrulla manual y se ha definido una posición final para el perfil de patrulla, la cámara vuelve a esta posición.

Añadir un perfil de patrulla

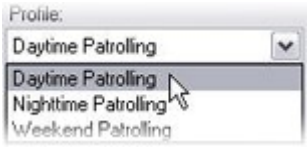
Antes de poder trabajar con las patrullas, debe especificar al menos dos posiciones preestablecidas para la cámara en la pestaña **Valores preestablecidos**, consulte Añadir una posición preestablecida (tipo 1).

1. En el panel **Navegación del sitio**, seleccione **Dispositivos** y a continuación seleccione **Cámaras**.
2. Seleccione la cámara PTZ correspondiente en el panel **Generalidades**.
3. En la pestaña **Patrulla**, haga clic en **Añadir**. Aparece el cuadro de diálogo **Añadir perfil**.
4. En el cuadro de diálogo **Añadir perfil**, especifique un nombre para el perfil de patrulla.
5. Haga clic en **Aceptar**. El botón se desactiva si el nombre no es único.

El nuevo perfil de patrulla se añade a la lista de **Perfiles**. Ahora puede especificar las posiciones preestablecidas y otros ajustes para el perfil de patrulla.

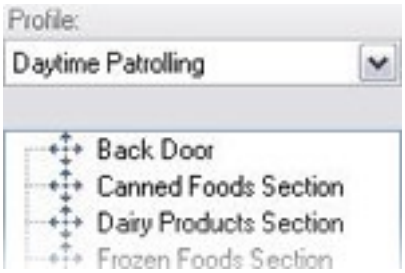
Especificar posiciones predefinidas en un perfil de vigilancia

1. En el panel **Navegación del sitio**, seleccione **Dispositivos** y a continuación seleccione **Cámaras**.
2. Seleccione la cámara PTZ correspondiente en el panel **Generalidades**.
3. En la pestaña **Vigilancia**, seleccione el perfil de vigilancia en la lista **Perfil**:



4. Haga clic en **Añadir**.
5. En el cuadro de diálogo **Seleccionar ajuste predefinido de PTZ**, seleccione las posiciones predefinidas para su perfil de vigilancia:

6. Haga clic en **Aceptar**. Las posiciones predefinidas seleccionadas se añaden a la lista de posiciones predefinidas para el perfil de vigilancia:



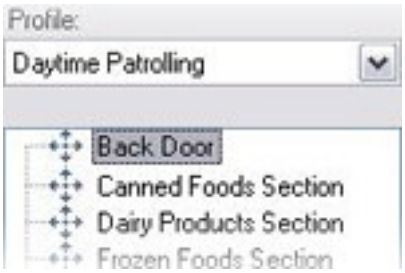
7. La cámara utiliza la posición predefinida en la parte superior de la lista como la primera parada cuando vigila de acuerdo con el perfil de vigilancia. La posición predefinida en la segunda posición desde arriba es la segunda parada y así sucesivamente.

Especificar el tiempo en cada posición predefinida

Al vigilar, de forma predeterminada la cámara PTZ permanece durante 5 segundos en en cada posición predefinida especificada en el perfil de vigilancia.

Para cambiar el número de segundos:

1. En el panel **Navegación del sitio**, seleccione **Dispositivos** y a continuación seleccione **Cámaras**.
2. Seleccione la cámara PTZ correspondiente en el panel **Generalidades**.
3. En la pestaña **Vigilancia**, seleccione el perfil de vigilancia en la lista **Perfil**.
4. Seleccione la posición preestablecida para la que quiere cambiar la hora:



5. Especifique el tiempo en el campo **Tiempo en posición (s)**.
6. Si es necesario, repítalo para las otras posiciones predefinidas.

Personalizar transiciones (PTZ)

Por defecto, el tiempo necesario para mover la cámara de una posición preestablecida a otra, conocido como **transición**, se estima en tres segundos. Durante este tiempo, la detección de movimiento está desactivada por defecto en la cámara, ya que de lo contrario es probable que se detecte un movimiento irrelevante mientras la cámara se mueve entre los valores preestablecidos.

Solo puede personalizar la velocidad de las transiciones si su cámara admite la exploración PTZ y es del tipo en el que las posiciones preestablecidas están configuradas y almacenadas en el servidor de su sistema (cámara PTZ de tipo 1). De lo contrario, el control deslizante de la **Velocidad** aparece en gris.

Puede personalizar lo siguiente:

- El tiempo de transición estimado
- La velocidad con la que se mueve la cámara durante una transición

Para personalizar las transiciones entre los diferentes valores preestablecidos:

1. En el panel **Navegación del sitio**, seleccione **Dispositivos** y a continuación seleccione **Cámaras**.
2. Seleccione la cámara PTZ correspondiente en el panel **Generalidades**.
3. En la pestaña **Patrulla**, seleccione el perfil de patrulla en la lista **Perfil** .
4. Seleccione la casilla **Personalizar transiciones**.

   Las indicaciones de transición se añaden a la lista de posiciones preestablecidas.
5. En la lista, seleccione la transición.

6. Especifique el tiempo de transición estimado (en número de segundos) en el campo **Tiempo previsto (seg)**.

7. Use el deslizador de **Velocidad** para especificar la velocidad de transición. Cuando el deslizador está en su posición más a la derecha, la cámara se mueve con su velocidad predeterminada. Cuanto más mueva el deslizador hacia la izquierda, más lentamente se moverá la cámara durante la transición seleccionada.
8. Repita la operación según sea necesario para otras transiciones.

Especificar una posición final al realizar la vigilancia

Puede especificar que la cámara debe moverse a una posición predefinida concreta cuando la vigilancia según el perfil de vigilancia seleccionado finalice.

1. En el panel **Navegación del sitio**, seleccione **Dispositivos** y a continuación seleccione **Cámaras**.
2. Seleccione la cámara PTZ correspondiente en el panel **Generalidades**.
3. En la pestaña **Vigilancia**, en a lista **Perfil**, seleccione el perfil de vigilancia relevante.
4. Seleccione la casilla de diálogo **Ir a la posición específica al terminar**. Esto abre el cuadro de diálogo **Seleccionar ajuste predefinido**.
5. Seleccione la posición final y haga clic en **Aceptar**.

   > Puede seleccionar cualquiera de las posiciones predefinidas de la cámara como la posición final, no está limitado a las posiciones predefinidas utilizadas en el perfil de vigilancia.

6. La posición final seleccionada se añade a la lista de perfiles.

Cuando termina la vigilancia según el perfil de vigilancia seleccionado, la cámara se mueve a la posición final especificada.

Reservar y liberar sesiones de PTZ

Dependiendo de su sistema de vigilancia, puede reservar sesiones de PTZ.

Los administradores con permisos 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.

Es posible operar la cámara en una sesión PTZ reservada desde XProtect Smart Client y Management Client.

La reserva de una sesión PTZ puede ser útil si le urge aplicar actualizaciones a cualquier cámara PTZ, o hacerle el mantenimiento, o a sus valores preestablecidos sin ser interrumpido por otros usuarios.

Reservar una sesión de PTZ

1. En el panel **Navegación del sitio**, seleccione **Dispositivos** y a continuación seleccione **Cámaras**.
2. Seleccione la cámara PTZ correspondiente en el panel **Generalidades**.
3. Seleccione la sesión de PTZ en la pestaña **Valores preestablecidos** y haga clic en **Reservado**.

> No puede iniciar una sesión de PTZ reservada si un usuario con una prioridad más elevada que la suya controla la cámara o si otro usuario ya ha reservado la cámara.

Liberar una sesión PTZ

El botón **Liberar** le permite liberar la sesión actual de PTZ para que otro usuario pueda controlar la cámara. Cuando hace clic en **Liberar**, la sesión de PTZ termina inmediatamente y estará disponible para que el primer usuario opere la cámara.

Los administradores asignados con el permiso de seguridad **Liberar sesión PTZ** tienen los permisos para liberar la sesión PTZ reservada de otros usuarios en cualquier momento. Esto puede, por ejemplo, ser útil en ocasiones en las que necesita mantener la cámara PTZ o sus valores preestablecidos, o si otros usuarios han bloqueado accidentalmente la cámara en situaciones urgentes.

Especificar tiempos de espera para sesiones de PTZ

Los usuarios de Management Client y XProtect Smart Client con los permisos de usuario necesarios pueden interrumpir manualmente el patrullaje de las cámaras PTZ.

Puede especificar cuánto tiempo debe transcurrir antes de que se reanude la vigilancia normal para todas las cámaras PTZ en su sistema:

1. Seleccione **Herramientas** > **Opciones**.
2. En la pestaña **General** de la ventana **Opciones**, seleccione la cantidad de tiempo en:
    - Lista **Tiempo de espera para sesiones manuales de PTZ** (el valor predeterminado es 15 segundos).
    - Lista **Tiempo de espera para poner en pausa las sesiones de vigilancia** (el valor predeterminado es 10 minutos).
    - Lista **Tiempo de espera para sesiones de PTZ reservadas** (el valor predeterminado es 1 hora).

    Los ajustes se aplican a todas las cámaras PTZ de su sistema.

Puede cambiar los tiempos de espera individualmente para cada cámara.

1. En el panel **Navegación por el sitio**, haga clic en **Cámara**.
2. En el panel Descripción general, seleccione la cámara.
3. En la pestaña **Valores preestablecidos**, seleccione la cantidad de tiempo en:
    - Lista **Tiempo de espera para la sesión manual de PTZ** (el valor predeterminado es 15 segundos).
    - Lista **Tiempo de espera para poner en pausa la sesión de vigilancia** (el valor predeterminado es 10 minutos).
    - Lista **Tiempo de espera para sesión de PTZ reservada** (el valor predeterminado es 1 hora).

    Los ajustes se aplican solo a esta cámara.

Dispositivos - Eventos para reglas

Añadir o eliminar un evento para un dispositivo

Añadir un evento

1. En el panel **Generalidades**, seleccione un dispositivo.
2. Seleccione la pestaña **Eventos** y haga clic en **Añadir**. Esto abre la ventana **Seleccionar evento del driver**.
3. Seleccione un evento. Solo puede seleccionar un evento a la vez.
4. Si desea ver una lista completa de todos los eventos, permitiéndole añadir eventos que ya han sido añadidos, seleccione **Mostrar eventos ya añadidos**.
5. Haga clic en **Aceptar**.
6. En la barra de herramientas, haga clic en **Guardar**.

Eliminar un evento

Cuando elimina un evento, afecta a todas las reglas que lo utilizan.

1. En el panel **Generalidades**, seleccione un dispositivo.
2. Seleccione la pestaña **Eventos** y haga clic en **Eliminar**.

Especificar las propiedades del evento

Puede especificar las propiedades de cada evento que haya añadido. El número de propiedades depende del dispositivo y del evento. Para que el evento funcione como es debido, debe especificar algunas o todas las propiedades de forma idéntica tanto en el dispositivo como en la pestaña **[Eventos]**.

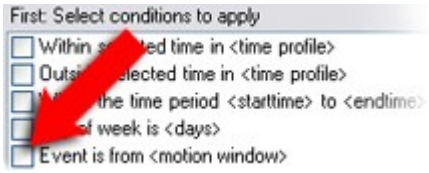
Usar varias instancias de un evento

Para poder especificar diferentes propiedades para distintas instancias de un evento, puede añadir un evento más de una vez.

El siguiente ejemplo es específico para las cámaras.

Ejemplo: Ha configurado la cámara con dos ventanas de movimiento, llamadas A1 y A2. Ha añadido dos instancias del evento Movimiento Iniciado (HW). En las propiedades de una instancia, ha 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 utilice el evento en una regla, puede especificar que el evento debe basarse en el movimiento detectado en una ventana de movimiento específica para que la regla se active:



Dispositivos - Eventos para reglas

Habilitar/deshabilitar la máscara de privacidad

La función de máscara de privacidad está desactivada por defecto.

Para habilitar/deshabilitar la función de máscara de privacidad para una cámara:

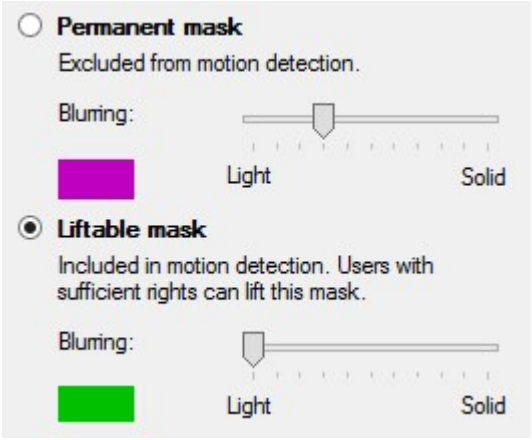
1. En el panel **Navegación del sitio**, seleccione **Dispositivos**.
2. Seleccione el dispositivo de cámara correspondiente en el panel **Generalidades**.
3. En la pestaña **Máscara de privacidad**, active o desactive la casilla **Máscara de privacidad**.

> 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, deberá redefinirlas en el sitio central.

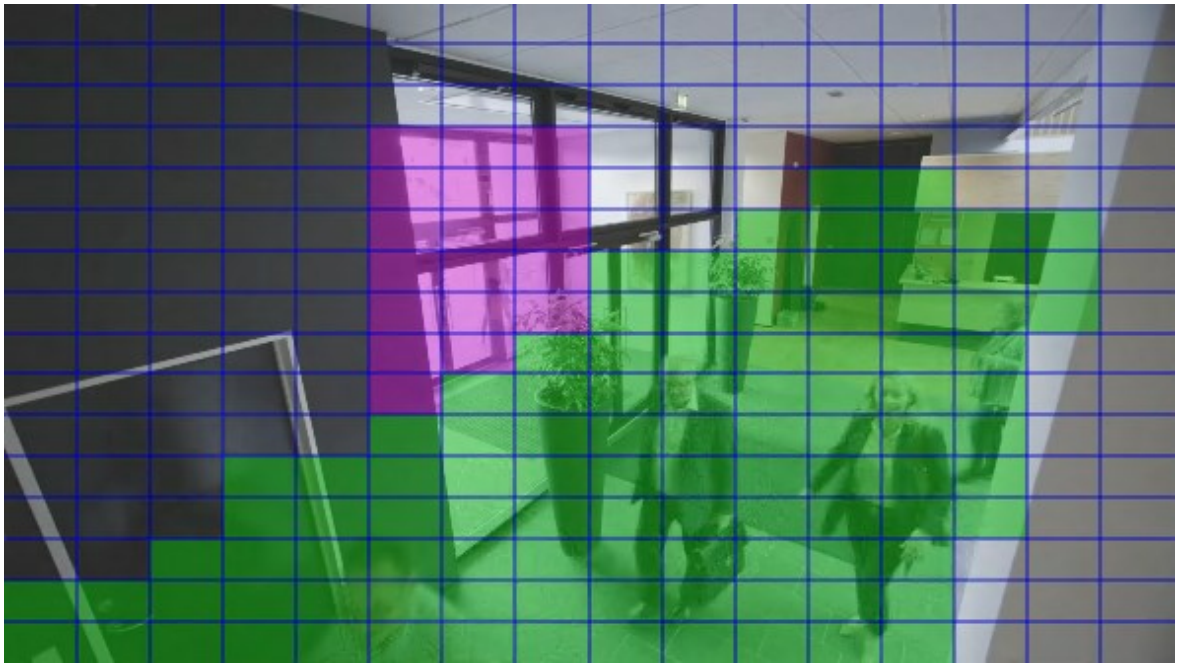
Definir las máscaras de privacidad

Cuando habilita la función de máscara de privacidad en la pestaña de **Máscara de privacidad**, se aplica una cuadrícula a la vista previa de la cámara.

1. En el panel **Navegación del sitio**, seleccione **Dispositivos**.
2. Seleccione la cámara correspondiente en el panel **Generalidades**.
3. En la pestaña **Máscara de privacidad**, para cubrir un área con una máscara de privacidad, seleccione primero **Máscara permanente** o **Máscara elevable** para definir si desea una máscara de privacidad permanente o elevable.



4. Arrastre el puntero del ratón sobre la vista previa. Haga clic con el botón izquierdo para seleccionar una celda de la cuadrícula. Haga clic con el botón derecho del ratón para borrar una celda de la cuadrícula.
5. Puede definir tantas áreas de máscara de privacidad como sea necesario. Las zonas con máscaras de privacidad permanentes aparecen en color púrpura y las áreas con máscaras de privacidad levantables en color verde.



6. Defina cómo debe aparecer el recubrimiento de las zonas en el vídeo cuando se muestre en los clientes. Utilice los controles deslizantes para pasar de un ligero desenfoque a una máscara totalmente no transparente.

   Las máscaras de privacidad permanentes también aparecen en la pestaña **Movimiento**.

7. En XProtect Smart Client, compruebe que las máscaras de privacidad aparecen tal y como las ha definido.

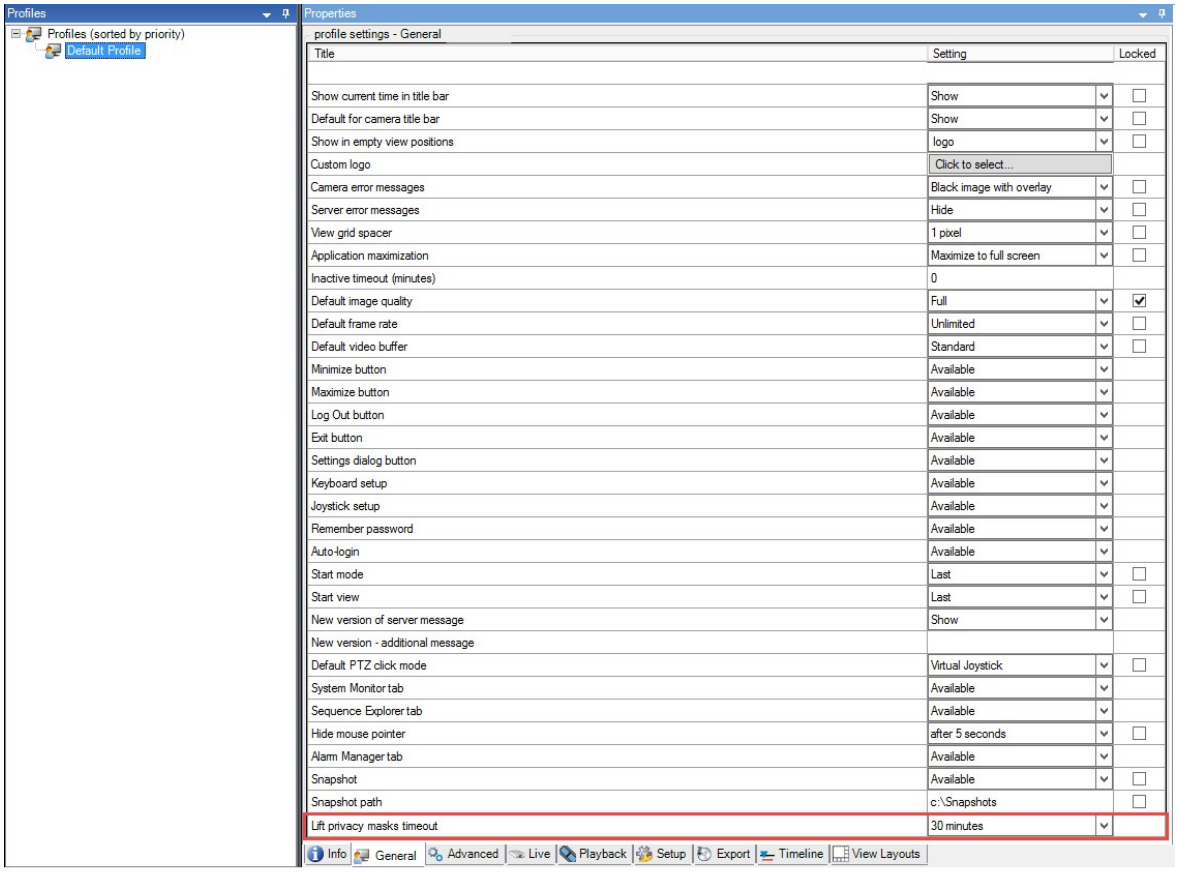
Cambiar el tiempo de espera de las máscaras de privacidad levantadas

Por defecto, las máscaras de privacidad se levantan durante 30 minutos en XProtect Smart Client y después se aplican automáticamente, pero puede cambiarlo.

Cuando cambie el tiempo de espera, recuerde hacerlo para el perfil de Smart Client asociado al cometido que tiene el permiso para elevar las máscaras de privacidad.

Para cambiar el tiempo de espera:

1. En **Perfiles Smart Client**, seleccione el perfil correspondiente Smart Client.
2. En la pestaña **General**, ubique **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**.

Dar permiso a los usuarios para levantar las máscaras de privacidad

Por defecto, ningún usuario tiene permisos para levantar las máscaras de privacidad en XProtect Smart Client.

Para habilitar/deshabilitar el permiso:

1. En el panel **Navegación del sitio**, seleccione **Seguridad** y a continuación seleccione **Cometidos**.
2. Seleccione el cometido al que desea dar permiso para levantar las máscaras de privacidad.
3. En la pestaña **Seguridad general**, seleccione **Cámaras**.
4. Seleccione la casilla **Permitir** para el permiso **Levantar máscaras de privacidad**.

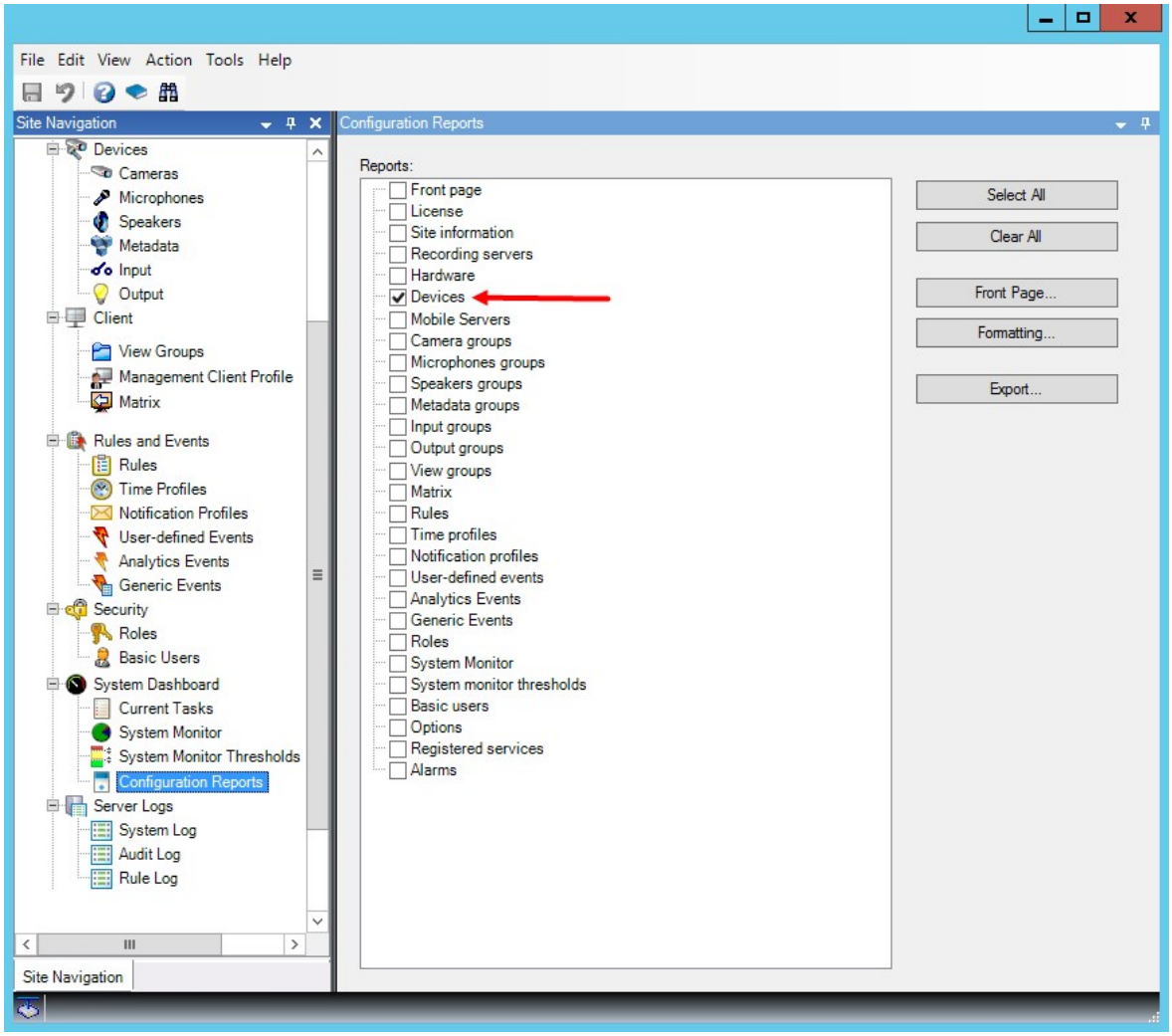
Los usuarios a los que se asigna este cometido, pueden levantar las máscaras de privacidad configuradas como elevables para sí mismos, así como autorizar la elevación para otros usuarios de XProtect Smart Client.

Crear un informe de su configuración de máscara de privacidad

El informe de los dispositivos incluye información sobre la configuración actual de máscara de privacidad de sus cámaras.

Para configurar un informe:

1. En el panel **Navegación del sitio**, seleccione **Panel del sistema**.
2. En **Informes de configuración**, seleccione el informe **Dispositivos**.



3. Si desea modificar el informe, puede cambiar la portada y el formato.
4. Haga clic en **Exportar**, y el sistema crea el informe como un archivo PDF.

Para obtener más información sobre los informes, consulte Imprimir un informe con la configuración del sistema en la página 307.

Clientes

Grupos de vistas (explicación)

El modo en que el sistema presenta vídeo desde una o varias cámaras en clientes se denomina una vista. Un grupo de vista es un contenedor para uno o varios grupos lógicos de estas vistas. En clientes, un grupo de vistas se presenta como una carpeta expandible desde la que los usuarios pueden seleccionar el grupo y la

vista que quieren ver:

Ejemplo de XProtect Smart Client: La flecha indica un grupo de vistas que contiene un grupo lógico (denominado Servicios), que, a su vez, contiene 3 vistas.

De forma predeterminada, cada rol que defina en Management Client también se crea como grupo de vistas. Al añadir un rol en Management Client, el rol aparece de forma predeterminada como un grupo de vistas para uso en clientes.

- Puede asignar un grupo de vistas basado en un rol a usuarios/grupos asignados al rol relevante. Puede cambiar estos permisos de grupo de vista configurando esto en los cometidos después
- Un grupo de vista basado en un rol lleva el nombre del rol.

  Ejemplo: Si crea un rol con el nombre **Personal de seguridad del edificio A**, aparece en XProtect Smart Client como un grupo de vistas llamado **Personal de seguridad del edificio A**.

  Además de los grupos de vistas que recibe al añadir cometidos, puede crear tantos grupos de vistas como quiera. También puede eliminar grupos de vistas, incluidos los creados automáticamente al añadir roles
- Aunque se cree un grupo de vistas cada vez que cree un nuevo cometido, los grupos de vistas no han de tener correspondencia en los cometidos. Puede añadir, cambiar el nombre o eliminar cualquiera de sus grupos de vistas si es necesrio

Si cambia el nombre de un Grupo de vistas, los usuarios clientes ya conectados deben cerrar sesión y volver a iniciar sesión antes de que el cambio de nombre sea visible.

Añadir un grupo de vistas

1. Haga clic con el botón derecho del ratón en **Grupos de vistas** y seleccione **Añadir grupo de vistas**. Esto abre el cuadro de diálogo **Añadir grupo de vista**.
2. Introduzca el nombre y una descripción opcional del nuevo grupo de vistas y haga clic en **Aceptar**.

Ningún cometido puede utilizar el grupo de vistas recién añadido hasta que haya especificado dichos permisos. Si ha especificado los cometidos que pueden utilizar el grupo de vistas recién añadido, los usuarios clientes que ya estén conectados y que tengan los cometidos correspondientes deberán cerrar la sesión e iniciarla de nuevo antes de poder ver el grupo de vistas.

Perfiles Smart Client

Añadir y configurar un perfil Smart Client

Debe crear un perfil antes de poder configurarlo Smart Client.

1. Haga clic con el botón derecho en **Smart Client Perfiles**.
2. Seleccione **Añadir Smart Client Perfil**.
3. En el cuadro de diálogo **Añadir perfil Smart Client**, introduzca un nombre y una descripción del nuevo perfil y haga clic en **Aceptar**.
4. En el panel **Generalidades** haga clic en el perfil que ha creado para configurarlo.
5. Ajuste la configuración en una, varias o todas las pestañas disponibles y haga clic en **OK**.

Copiar un perfil Smart Client

Si tiene un perfil con ajustes Smart Client o permisos complicados y necesita un perfil similar, puede ser más fácil copiar un perfil ya existente y hacer pequeños ajustes en la copia que crear un nuevo perfil desde cero.

1. Haga clic en **Perfiles Smart Client**, haga clic con el botón derecho en el panel **Generalidades**, seleccione **Copiar Perfil Smart Client**.
2. En el cuadro de diálogo que aparece, dé al perfil copiado un nuevo nombre único y una descripción. Haga clic en **Aceptar**.
3. En el panel **Generalidades** haga clic en el perfil que acaba de crear para configurarlo. Esto se hace ajustando la configuración en una, varias o todas las pestañas disponibles. Haga clic en **Aceptar**.

Crear y configurar perfiles, cometidos y perfiles temporales Smart Client

Cuando se trabaja con perfiles Smart Client, es importante entender la interacción entre perfiles Smart Client, cometidos y perfiles temporales:

- Los perfiles Smart Client se ocupan de la configuración de los permisos de los usuarios en XProtect Smart Client
- Los cometidos se ocupan de los ajustes de seguridad en los clientes, MIP SDK y más
- Los perfiles temporales se ocupan de los aspectos temporales de los dos tipos de perfiles

Juntas, estas tres características proporcionan un control único y posibilidades de personalización con respecto a los permisos de los usuarios de XProtect Smart Client.

Ejemplo: Necesita un usuario en su configuración XProtect Smart Client que solo pueda ver vídeo en directo (sin reproducción) de las cámaras seleccionadas, y solo durante las horas normales de trabajo (de 8.00 a 16.00). Una forma de configurarlo podría ser la siguiente:

1. Cree un perfil Smart Client y llámelo, por ejemplo, **Solo en directo**.
2. Especifique los ajustes necesarios para el directo/reproducción en **Solo Directo** .
3. Cree un perfil temporal y llámelo, por ejemplo, **Solo de día**.
4. Especifique el período de tiempo necesario en **Solo de Día**.
5. Cree un nuevo cometido y llámelo, por ejemplo, **Guardia (Cámaras seleccionadas)**.
6. Especifique qué cámaras puede utilizar la **Guardia (Cámaras seleccionadas)**.
7. Asigne el perfil Smart Client **Solo en directo** y el perfil temporal **Solo de día** al cometido **Guardia (Cámaras seleccionadas)** para conectar los tres elementos.

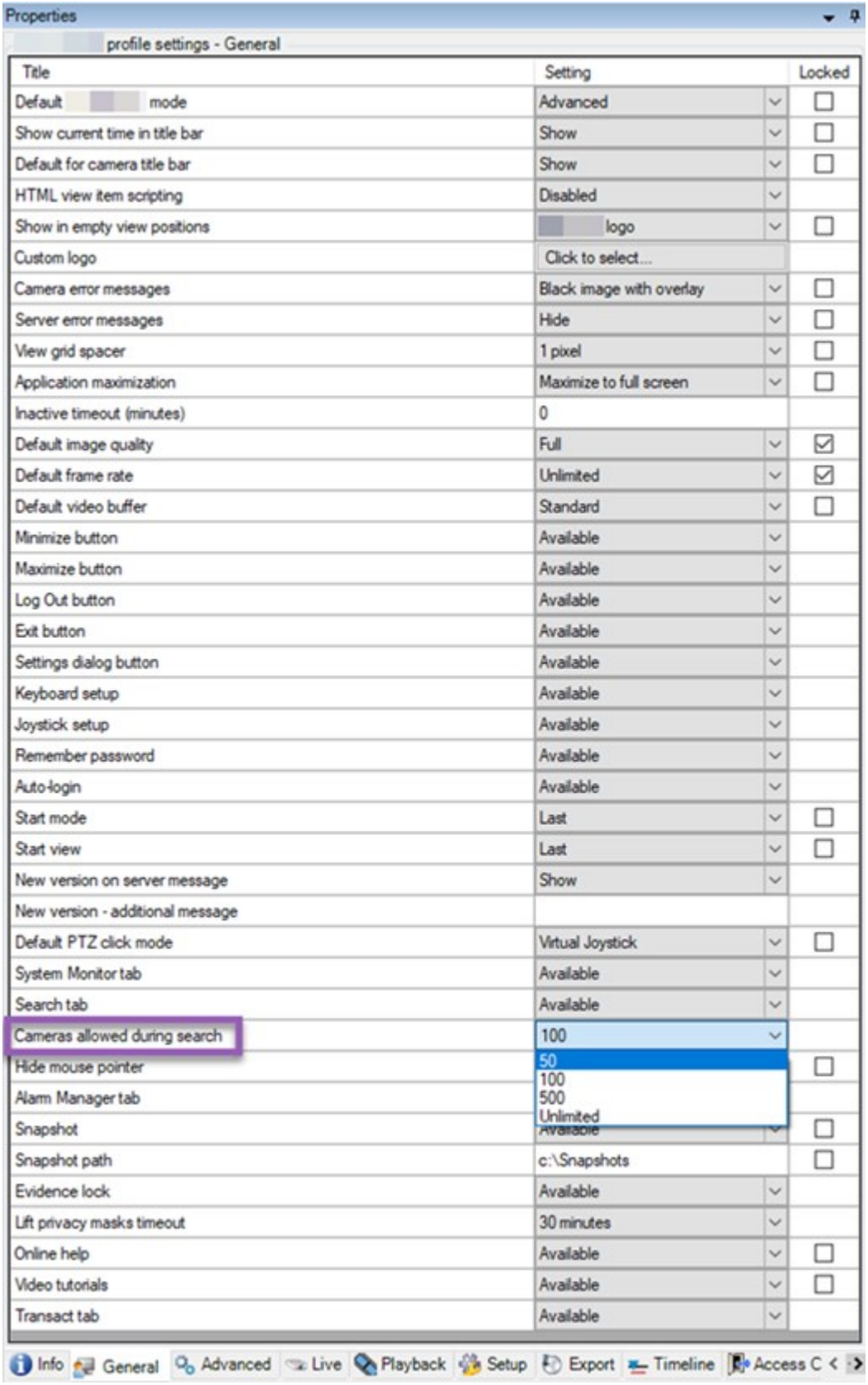
Ahora tiene una mezcla de las tres características que crea el resultado deseado y le permite un fácil ajuste y puesta a punto. Puede hacer la configuración en un orden diferente, por ejemplo, creando primero el cometido y después el perfil Smart Client y el perfil temporal, o en cualquier otro orden que prefiera.

Establecer el número de cámaras permitidas durante la búsqueda

Puede configurar cuántas cámaras pueden añadir los operadores a una búsqueda en XProtect Smart Client. El valor por defecto es **100**. Si se supera el límite de la cámara, el operador recibe una advertencia.

1. En XProtect Management Client, expanda **Cliente** > **Smart Client Perfiles**.
2. Seleccione el perfil correspondiente.

3. Haga clic en la pestaña **General**.


Properties
profile settings - General
Title
Setting
Locked
Default mode
Advanced
Show current time in title bar
Show
Default for camera title bar
Show
HTML view item scripting
Disabled
Show in empty view positions
logo
Custom logo
Click to select...
Camera error messages
Black image with overlay
Server error messages
Hide
View grid spacer
1 pixel
Application maximization
Maximize to full screen
Inactive timeout (minutes)
0
Default image quality
Full
Default frame rate
Unlimited
Default video buffer
Standard
Minimize button
Available
Maximize button
Available
Log Out button
Available
Exit button
Available
Settings dialog button
Available
Keyboard setup
Available
Joystick setup
Available
Remember password
Available
Auto-login
Available
Start mode
Last
Start view
Last
New version on server message
Show
New version - additional message
Default PTZ click mode
Virtual Joystick
System Monitor tab
Available
Search tab
Available
Cameras allowed during search
100
50
100
500
Unlimited
Hide mouse pointer
Alarm Manager tab
Snapshot
Snapshot path
c:\Snapshots
Evidence lock
Available
Lift privacy masks timeout
30 minutes
Online help
Available
Video tutorials
Available
Transact tab
Available
Info
General
Advanced
Live
Playback
Setup
Export
Timeline
Access C

4. En las **Cámaras** permitidas durante la búsqueda, seleccione uno de estos valores:
    - **50**
    - **100**
    - **500**
    - **Ilimitado**
5. Guarde sus cambios.

Cambiar los ajustes de exportación por defecto

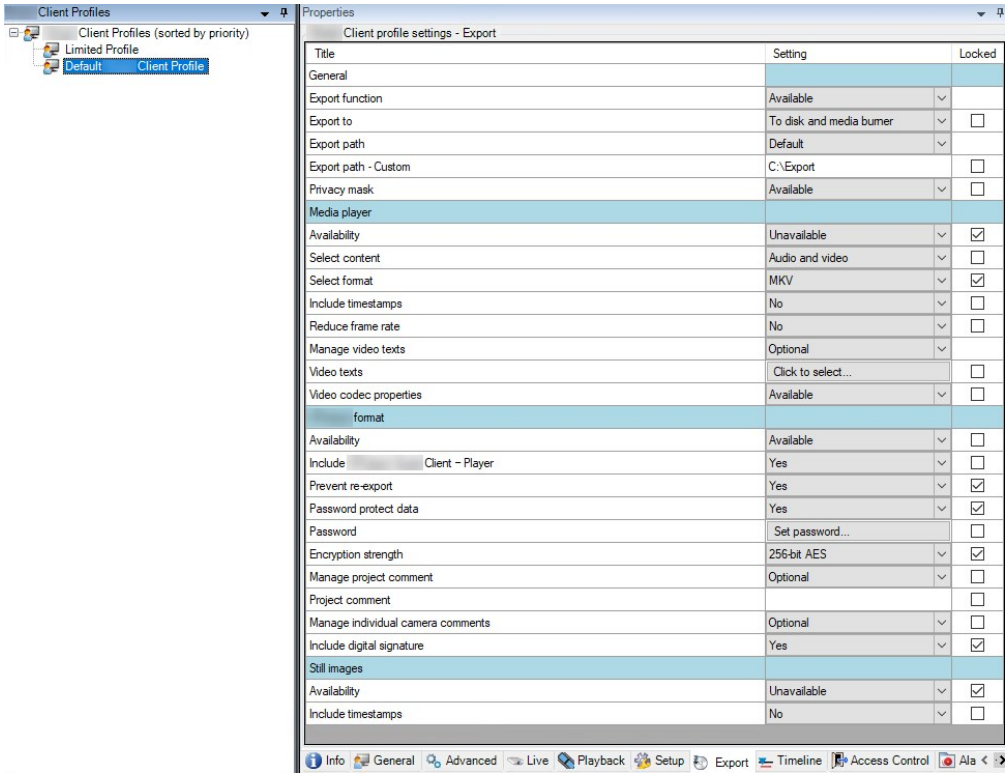
Cuando instala su sistema VMS XProtect, los ajustes de exportación por defecto que define las opciones de exportación en XProtect Smart Client está restringida para garantizar el máximo nivel de seguridad. Puede cambiar estos ajustes para dar a los operadores más opciones.

Ajustes por defecto

- Únicamente el formato XProtect está disponible
    - Se evita la reexportación
    - Las exportaciones están protegidas mediante contraseña
    - Cifrado AES de 256 bits
    - Se añaden las firmas digitales
- No es posible exportar a formato MKV o AVI
- No es posible exportar imágenes fijas

Pasos:

1. En XProtect Management Client, expanda **Cliente** > **Smart Client Perfiles**.
2. Seleccione **Perfil por defecto Smart Client**.
3. En el panel **Propiedades** seleccione la pestaña **Exportción**.



4. Para que un formato restringido esté disponible en XProtect Smart Client, busque el ajuste y seleccione **Disponible**.
5. Para habilitar a los operadores para que cambien un ajuste en XProtect Smart Client, desactive la casilla **Bloqueado** junto al ajuste correspondiente.
6. Si es pertinente, cambie otros ajustes.
7. (opcional) Inicie sesión en XProtect Smart Client para verificar que se han aplicado sus ajustes.

Perfiles Management Client

Añadir y configurar un perfil Management Client

Si no desea utilizar el perfil por defecto, puede crear un perfil Management Client antes de configurarlo.

1. Haga clic con el botón derecho en **Perfiles Management Client**.
2. Seleccione **Añadir Management Client Perfil**.
3. En el cuadro de diálogo **Añadir perfil Management Client**, introduzca un nombre y una descripción del nuevo perfil y haga clic en **Aceptar**.
4. En el panel **Generalidades** haga clic en el perfil que ha creado para configurarlo.
5. En la pestaña **Perfil**, seleccione o borre la funcionalidad del perfil Management Client.

Copiar un perfil Management Client

Si tiene un perfil Management Client con ajustes que le gustaría reutilizar, puede copiar un perfil ya existente y hacer pequeños ajustes en la copia en lugar de crear un nuevo perfil desde cero.

1. Haga clic en **Management Client Perfil**, haga clic con el botón derecho en el panel **Generalidades**, seleccione **Copiar Management Client Perfil**.
2. En el cuadro de diálogo que aparece, dé al perfil copiado un nuevo nombre único y una descripción. Haga clic en **Aceptar**.
3. En el panel **Generalidades**, haga clic en el perfil y vaya a la pestaña **Información** o a la pestaña **Perfil** para configurar el perfil.

Gestionar la visibilidad de la funcionalidad de un perfil de Management Client

Asocie perfiles Management Client con los cometidos para limitar la interfaz de usuario para representar la funcionalidad disponible para cada cometido de administrador.

Asociar un perfil de Management Client con un cometido

1. Expanda el nodo de **Seguridad** y haga clic en **Cometidos**.
2. En la pestaña **Información** en la ventana **Ajustes de cometido**, asocie un perfil con un cometido. Si desea más información, consulte la pestaña Información (cometidos).

Gestionar el acceso general a la funcionalidad del sistema para un cometido

Management Client los perfiles solo manejan la representación visual de la funcionalidad del sistema, no el acceso real a ella.

Para gestionar el acceso general a la funcionalidad del sistema para un cometido:

1. Expanda el nodo de **Seguridad** y haga clic en **Cometidos**.
2. Haga clic en la pestaña **Seguridad general** y seleccione las casillas de verificación correspondientes. Si desea más información, consulte Pestaña Seguridad global (roles) en la página 540.

En la pestaña **Seguridad general**, asegúrese de habilitar el permiso de seguridad **Conectar** para conceder a todos los cometidos el acceso al Management Server.

Aparte del cometido de administrador incorporado, solo los usuarios asociados a un cometido al que se le hayan concedido permisos de **Gestionar seguridad** para el servidor de gestión en la pestaña de **Seguridad general**, pueden añadir, editar y eliminar perfiles Management Client.

Limitar la visibilidad de la funcionalidad de un perfil

Puede cambiar la configuración de la visibilidad de todos los elementos Management Client. Por defecto, el perfil Management Client puede ver todas las funcionalidades en el Management Client.

1. Despliegue el nodo Cliente y haga clic en Perfiles Management Client.
2. Seleccione un perfil y haga clic en la pestaña Perfil.
3. Desmarque las casillas de verificación de la funcionalidad correspondiente para eliminar la funcionalidad de forma visual de Management Client para cualquier usuario de Management Client con un cometido asociado a este perfil Management Client.

Matrix

Matrix y Matrix destinatarios (explicación)

Matrix es una función para distribuir vídeo de manera remota.

Un destinatario de Matrix es un ordenador con XProtect Smart Client, que se define como un destinatario de Matrix en Management Client.

Si utiliza Matrix, puede enviar automáticamente vídeo desde cualquier cámara de la red de su sistema a cualquier destinatario de Matrix que se esté ejecutando.

Para ver una lista de destinatarios de Matrix añadidos en Management Client, expanda **Cliente** en el panel **Navegación por el sitio**, luego seleccione **Matrix**. Una lista de configuraciones de Matrix se muestra en el panel **Propiedades**.

En Management Client, debe añadir a cada destinatario de Matrix para recibir vídeo desencadenado por Matrix.

Definir reglas que envían vídeo a destinatarios de Matrix

Para enviar vídeo a destinatarios de Matrix, debe incluir al destinatario de Matrix en una regla que desencadene la transmisión de vídeo al destinatario de Matrix relacionado. Para hacerlo:

1. En el panel **Navegación por el sitio**, expanda **Reglas y eventos** > **Reglas**. Haga clic con el botón derecho del ratón en **Reglas** para abrir el asistente **Gestionar regla**. En el primer paso, seleccione un tipo de regla y en el segundo paso, una condición.
2. En el paso 3 de **Gestionar regla** (**Paso 3: Acciones**), seleccione **Establecer Matrix para ver la acción la acción de <dispositivos>**.
3. Haga clic en el enlace Matrix de la descripción inicial de la regla.
4. En el cuadro de diálogo **Seleccionar Matrix Configuración**, seleccione el destinatario de Matrix relevante y haga clic en **Aceptar**.
5. Haga clic en el enlace **dispositivos** de la descripción inicial de la regla y seleccione de qué cámaras quiere enviar vídeo al destinatario de Matrix y, a continuación, haga clic en **Aceptar** para confirmar su selección.
6. Haga clic en **Terminar** si la regla está completa o defina si requiere acciones adcionales y/o una acción de parada.

Si elimina un destinatario de Matrix, cualquier regla que incluya al destinatario de Matrix deja de funcionar.

Añadir destinatarios de Matrix

Para añadir un destinatario de Matrix existente en Management Client:

1. Expanda **Clientes** y, a continuación, seleccione **Matrix**.
2. Haga clic con el botón derecho en **Configuraciones de Matrix** y seleccione **Añadir Matrix**.
3. Cumplimente los campos en el cuadro de diálogo **Añadir Matrix**.
    1. En el campo **Dirección**, introduzca la dirección IP o el nombre de host del destinatario de Matrix requerido.
    2. En el campo **Puerto**, introduzca el número de puerto utilizado por la instalación del destinatario de Matrix.
4. Haga clic en **Aceptar**.

Ahora puede utilizar el destinatario de Matrix en reglas.

El sistema no verifica que el número de puerto o la contraseña especificados sean correctos o que el número de puerto, la contraseña o el tipo especificados correspondan al destinatario de Matrix real. Asegúrese de introducir la información correcta.

Enviar el mismo vídeo a varias vistas de XProtect Smart Client

Puede enviar el mismo vídeo a Matrix posiciones en varias de las vistas de XProtect Smart Client, siempre que las Matrix posiciones de las vistas compartan el mismo número de puerto y contraseña:

1. En XProtect Smart Client, cree las vistas relevantes y las posiciones de Matrix que compartan el mismo número de puerto y contraseña.
2. En Management Client, añada el XProtect Smart Client relevante como destinatario de Matrix.
3. Puede incluir al destinatario de Matrix en una regla.

Reglas y eventos

Añadir reglas

Al añadir reglas, le guía el asistente **Gestionar regla**, que solo recoge las opciones relevantes.

Garantiza que los elementos necesarios no falten en una regla. Basándose en el contenido de su regla, automáticamente sugiere acciones de parada adecuadas, que es lo que debe ocurrir cuando la regla deja de aplicarse, lo que garantiza que no crea de forma no intencionada una regla interminable.

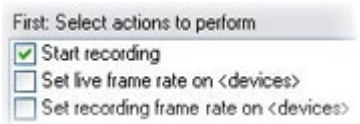
Eventos

Al añadir una regla basada en eventos, puede seleccionar distintos tipos de eventos.

- Consulte Descripción general de eventos para obtener información general y una descripción de los tipos de evento que puede seleccionar.

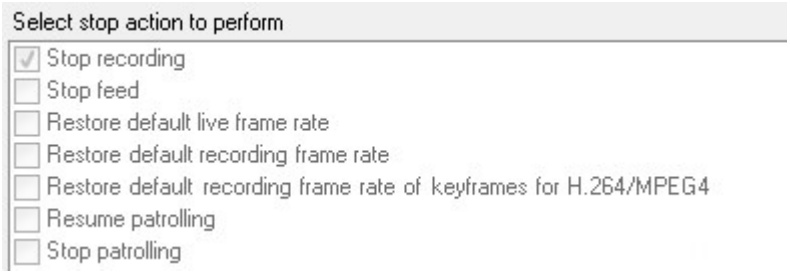
Acciones y acciones de parada

Al añadir reglas, puede seleccionar acciones distintas.



Algunas de las acciones requieren una acción de parada. Por ejemplo, si selecciona la acción **Iniciar grabación**, la grabacion comienza y potencialmente continúa de forma indefinida. Como resultado, la acción **Iniciar grabación** tiene una acción de parada obligatoria denominada **Detener grabación**.

El asistente **Gestionar regla** se asegura de que especifica acciones de parada cuando sea necesario:



Selección de acciones de parada. En el ejemplo, observe la acción de detener obligatoria (seleccionado, atenuado), las acciones de parada no relevantes (atenuado) y las acciones de parada opcionales (seleccionable).

- Consulte Acciones y acciones de parada para obtener una descripción general de acciones de inicio y parada que puede seleccionar.

Crear una regla

1. Haga clic con el botón derecho del ratón en el elemento **Reglas** > **Añadir regla**. Esto abre el asistente **Gestionar reglas**. El asistente le guía por la especificación de contenido de su perfil.
2. Especifique un nombre y una descripción de la regla nueva en los campos **Nombre** y **Descripción** respectivamente.
3. Seleccione el tipo relevante de condición para la regla: una regla que realiza una o más acciones cuando se produce un evento concreto o una regla que realiza una o más acciones cuando introduce un periodo de tiempo concreto.
4. Haga clic en **Siguiente** para ir al segundo paso del asistente. En el segundo paso del asistente, defina más condiciones para la regla.

5. Seleccione una o más condiciones, por ejemplo **El día de la semana es <día>**:

Dependiendo de sus selecciones, edite la descripción de la regla en la parte inferior de la ventana del asistente:

Haga clic en los elementos subrayados en **negrita y cursiva** para especificar su contenido exacto. Por ejemplo, hacer clic en el enlace **días** en nuestro ejemplo le permite seleccionar uno o más días de la semana en los que se debe aplicar la regla.

6. Después de haber especificado sus condiciones exactas, haga clic en **Siguiente** para pasar al paso siguiente del asistente y seleccione qué acciones debe cubrir la regla. Dependiendo del contenido y de la complejidad de su regla, puede tener que definir más pasos, como eventos de parada y acciones de parada. Por ejemplo, si una regla especifica que un dispositivo debe realizar una acción concreta durante un intervalo de tiempo, Jueves entre las 08.00 y las 10.30), el asistente puede pedirle que especifique qué ocurrir cuando finaliza ese intervalo de tiempo.
7. Su regla se activa, de forma predeterminada, una vez que la haya creado si se cumplen las condiciones de la regla. Si no quiere que la regla esté activa de inmediato, desactive la casilla de verificación **Activa**.
8. Haga clic en **Finalizar**.

Validar reglas

Puede validar el contenido de una regla individual o de todas las reglas a la vez. Al crear una regla, el asistente **Gestionar regla** se asegura de que todos los elementos de la regla son válidos.

Cuando una regla ha existido durante algún tiempo, uno o más elementos de la regla pueden haberse visto afectados por otra configuración, y es posible que la regla ya no funcione. Por ejemplo, si una regla se desencadena por un perfil temporal concreto, la regla no funciona si ha eliminado ese perfil temporal o si ya no tiene permisos en él Puede ser difícil conservar una descripción general de tales efectos de configuración no intencionados.

La validación de reglas le ayuda a hacer un seguimiento de qué reglas se han visto afectadas. La validación se realiza regla por regla y cada regla se valida por sí misma. No puede validar reglas entre sí, por ejemplo para ver si una regla entra en conflicto con otra regla, ni siquiera si utiliza la función **Validar todas las reglas**.

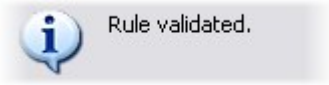
Validar una regla

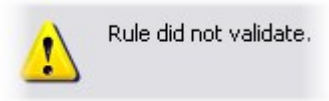
1. Haga clic en **Reglas** y seleccione la regla que quiere validar.
2. Haga clic con el botón derecho del ratón en la regla y haga clic en **Validar regla.**
3. Haga clic en **Aceptar**.

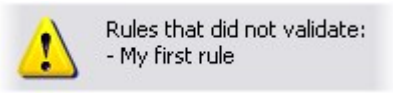
Validar todas las reglas

1. Haga clic con el botón derecho del ratón en el elemento **Reglas** y luego haga clic en **Validar todas las reglas**. .
2. Haga clic en **Aceptar**.

Un cuadro de diálogo le informa de si la(s) regla(s) se ha(n) validado correctamente o no. Si opta por validar más de una regla y y una o más reglas no tuvieron éxito, el cuadro de diálogo enumera los nombres de las reglas afectadas.







No puede validar si la configuración de requisitos fuera de la propia regla puede evitar que la regla funcione. Por ejemplo, una regla que especifica que la grabación debe tener lugar al detectar movimiento con una cámara concreta se valida si los elementos de la propia regla son correctos, incluso si la detección de movimiento, que se activa a nivel de cámara, no por medio de reglas, no se ha habilitado para la cámara relevante.

Editar, copiar y cambiar el nombre de una regla

1. En el panel **Descripción general**, haga clic con el botón derecho en la regla relevante.
2. Seleccione cualquiera:

   Editar regla o **Copiar regla** o **Cambiar nombre de regla**. Se abre el asistente **Gestionar reglas**.

3. Si selecciona **Copiar regla**, el asistente se abre y muestra una copia de la regla seleccionada. Haga clic en **Terminar** para crear una copia.
4. Si selecciona **Editar regla**, el asistente se abre y puede introducir cambios. Haga clic en **Terminar** para aceptar los cambios.
5. Si selecciona **Cambiar nombre de regla**, puede cambiar el nombre de la regla directamente en el texto del nombre de la regla.

Desactivar y activar una regla

El sistema aplica una regla tan pronto como se cumplan las condiciones de la regla, lo que significa que está activa. Si no quiere que una regla esté activa, puede desactivar la regla. Al desactivar la regla, el sistema no aplica la regla incluso aunque se aplique la condición de la regla. Más adelante, puede activar fácilmente una regla desactivada.

Desactivando una regla

1. En el panel **Descripción general**, seleccione la regla.
2. Desactive la casilla de verificación **Activo** en el panel **Propiedades**.
3. Haga clic en **Guardar** en la barra de herramientas.
4. Un icono con una x roja indica que la regla se ha desactivado en la lista **Reglas**:

Activación de una regla

Cuando quiera activar la regla de nuevo, seleccione la regla, seleccione la casilla de verificación **Activar** y guarde el ajuste.

Especificar un perfil temporal

1. En la lista **Perfiles temporales**, haga clic con el botón derecho en **Perfiles temporales** > **Añadir perfil temporal**. Esto abre la ventana **Perfil temporal**.
2. En la ventana **Perfil temporal**, introduzca el nombre del nuevo perfil temporal en el campo **Nombre**. Opcionalmente, introduzca una descripción del nuevo perfil temporal en el campo **Descripción**.
3. En el calendario de la ventana **Perfil temporal**, seleccione **Vista de días**, **Vista de semanas** o **Vista de meses** y, a continuación, haga clic con el botón derecho dentro del calendario y seleccione **Añadir una única hora** o **Añadir una hora recurrente**.

4. Cuando haya especificado los periodos de tiempo para su perfil de tiempo, haga clic en **Aceptar** en la ventana **Perfil temporal**. El sistema añade su perfil temporal nuevo a la lista **Perfiles temporales**. Si, más adelante, quiere editar o eliminar el perfil de tiempo, también lo hace desde la lista **Perfiles temporales**.

Añadir una sola hora

Al seleccionar **Añadir tiempo único**, aparece la ventana **Seleccionar tiempo**:

El formato de la fecha y la hora puede ser diferente en su sistema.

1. En la ventana **Seleccionar hora**, especifique **Hora de inicio** y **Hora de fin**. Si el tiempo debe cubrir el día entero, seleccione la casilla **Evento de todo el día**.
2. Haga clic en **Aceptar**.

Añadir una hora recurrente

Al seleccionar **Añadir tiempo recurrente**, aparece la ventana **Seleccionar tiempo recurrente**:

1. En la ventana **Seleccionar hora**, especifique el intervalo de tiempo, el patrón de recurrencia y el intervalo de recurrencia.
2. Haga clic en **Aceptar**.

Un perfil temporal puede contener varios periodos de tiempo. Si quiere que su perfil temporal contenga más periodos de tiempo, añada más tiempos únicos o recurrentes.

Tiempo recurrente

Cuando establezca que una acción se ejecute en una programación detallada y recurrente.

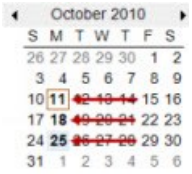
Por ejemplo:

- Cada semana, el martes, cada 1 hora(s) entre 15:00 y 15:30
- El día 15 cada 3 mes(es) a las 11:45
- Todos los días cada 1 hora(s) entre 15:00 y 19:00

La hora se basa en la configuración de la hora local del servidor en el que está instalado Management Client.

Editar un perfil temporal

1. En la lista **Perfiles temporales** del panel **Descripción general**, haga clic con el botón derecho del perfil temporal relevante y seleccione **Editar perfil temporal**. Esto abre la ventana **Perfil temporal**.
2. Edite el perfil temporal según sea necesario. Si ha realizado cambios en el perfil temporal, haga clic en **Aceptar** en la ventana **Perfil temporal**. Vuelve a la lista **Perfiles temporales**.



En la ventana **Información de perfiles temporales**, puede editar el perfil temporal según sea necesario. Recuerde que un perfil temporal puede contener más de un periodo de tiempo, y que los periodos de tiempo pueden ser recurrentes. La pequeña descripción general del mes en la esquina superior derecha puede ayudarle a tener una descripción general rápida de los periodos de tiempo que abarca el perfil temporal, ya que las fechas que contienen tiempos especificados se resaltan en negrita.

En este ejemplo, las fechas en negrita indican que ha especificado periodos de tiempo en varios días, y que ha especificado una hora recurrente los lunes.

Crear perfiles temporales de duración de día

1. Expanda la carpeta **Reglas y eventos** > **Perfiles temporales**.
2. En la lista **Perfiles temporales**, haga clic con el botón derecho en **Perfiles temporales** y seleccione **Añadir perfil temporal de duración de día**.
3. En la ventana **Perfil temporal de duración de día**, consulte la tabla de propiedades de debajo para rellenar la información necesaria. Para tratar con periodos de transición entre claridad y oscuridad, puede compensar la activación y desactivación del perfil. Las horas y el nombre de los meses se muestran en el idioma utilizando según los ajustes regionales y de idioma de su ordenador.
4. Para ver la ubicación de las coordenadas geográficas introducidas en un plano, haga clic en **Mostrar posición en el explorador**. Esto abre un navegador en el que puede ver la ubicación.
5. Haga clic en **Aceptar**.

Propiedades del perfil temporal de duración de día

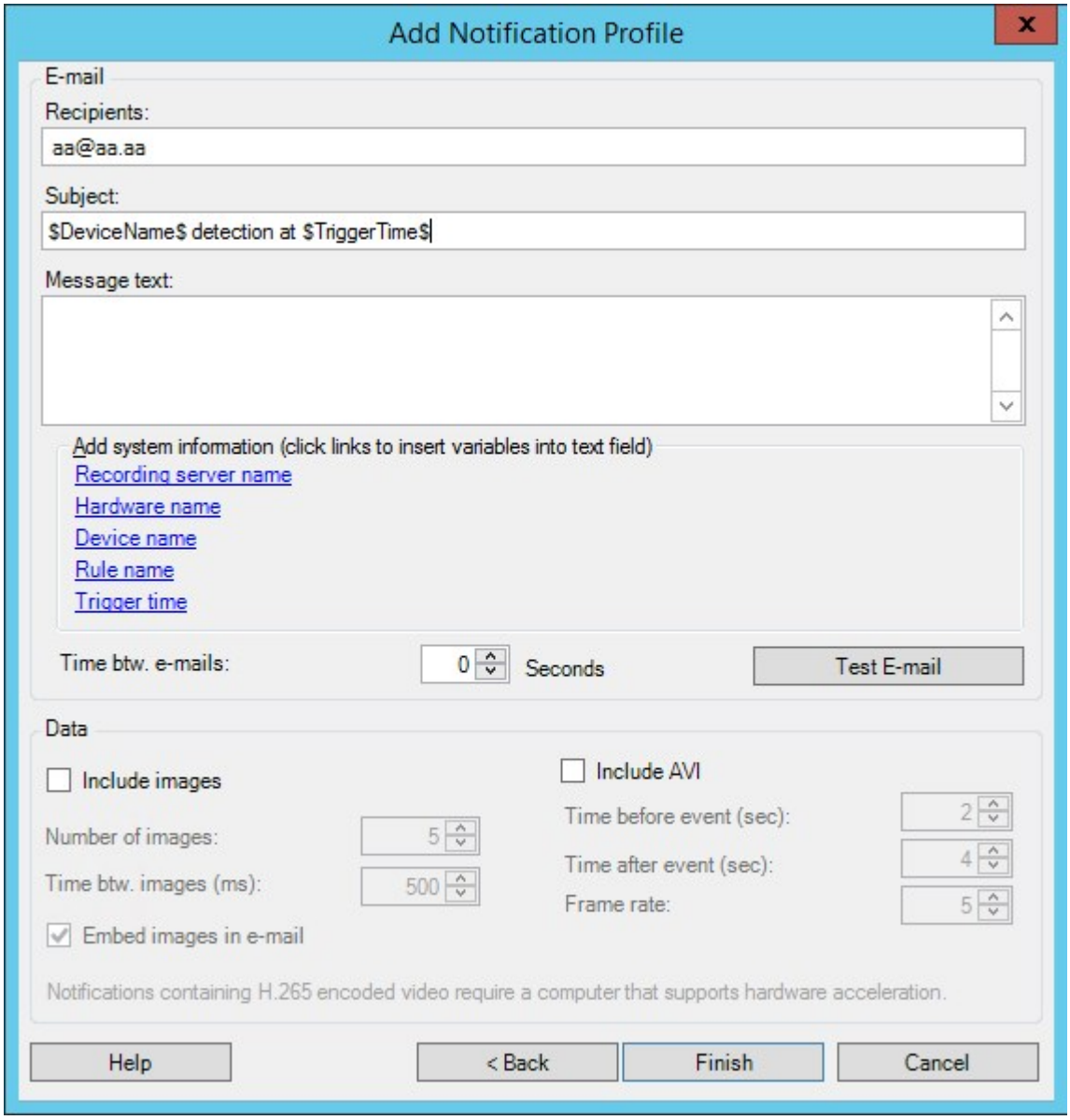
Nombre	Descripción
Nombre	El nombre del perfil.
Descripción	Una descripción del perfil (opcional).
Coordenadas GPS	Coordenadas geográficas que indican la ubicación física de la(s) cámara(s) asignada(s) al persil.
Compensación de amanecer	Número de minutos (+/-) por los que la activación del perfil se compensa con el amanecer.
Compensación de ocaso	Número de minutos (+/-) por los que la desactivación del perfil se compensa con el ocaso.
Zona horaria	Zona horaria que indica la ubicación física de la(s) cámara(s).

Añadir perfiles de notificación

Antes de poder crear perfiles de notificación, debe especificar ajustes del servidor de correo para las notificaciones de correo electrónico. Para obtener información adicional, consulte Requisitos para crear perfiles de notificación.

1. Expanda **Reglas y eventos**, haga clic con el botón derecho en **Perfiles de notificación** > **Añadir perfil de notificación**. Esto abre el asistente **Añadir perfil de notificaciones**.
2. Especifique un nombre y una descripción. Haga clic en **Siguiente**.

3. Especifique el destinatario, el asunto, el texto del mensaje y el tiempo entre correos electrónicos:



4. Para enviar una notificación de correo electrónico de prueba a los destinatarios especificados, haga clic en **Correo electrónico de prueba**.
5. Para incluir imágenes fijas previas a la alarma, seleccione **Incluir imágenes** y especifique el número de imágenes, el tiempo entre imágenes y si se deben incrustar o no imágenes en correos electrónicos.
6. Para incluir videoclips AVI, seleccione **Incluir AVI** y especifique el tiempo antes y después del evento y la velocidad de fotogramas.

> Las notificaciones que contienen vídeo codificado H.265 requieren un equipo que admita la aceleración de hardware.

7. Haga clic en **Finalizar**.

Desencadenar notificaciones de correo electrónico a partir de reglas

1. Haga clic con el botón derecho del ratón en el elemento **Reglas** y luego haga clic en > **Añadir regla** o **Editar regla**.
2. En el asistente **Gestionar regla**, haga clic en **Siguiente** para ir a la lista **Seleccionar acciones que realizar** y seleccione **Enviar notificación a <perfil>**.
3. Seleccione el perfil de notificación relevante y seleccione las cámaras de las que deben venir las grabaciones que se deben incluir en las notificaciones de correo electrónico del perfil de notificación.

No puede incluir grabaciones en las notificaciones de correo electrónico del perfil de notificación a menos que se esté grabando algo realmente. Si quiere imágenes fijas o videoclips AVI en las notificaciones de correo electrónico, verifique que la regla especifica que la grabación debe tener lugar. El siguiente ejemplo es de una regla que incluye tanto una acción de **Iniciar grabación** como una acción **Enviar notificación a**:

Añadir un evento definido por el usuario

> No importa cómo quiere utilizar los eventos definidos por el usuario, debe añadir cada evento definido por el usuario mediante el Management Client.

1. Expandir **Reglas y Eventos** > **Eventos definidos por el usuario**.
2. En el panel **Descripción general**, haga clic con el botón derecho en **Eventos** > **Añadir evento definido por el usuario**.

3. Introduzca un nombre para el nuevo evento definido por el usuario y haga clic en **Aceptar**. El evento definido por el usuario que acaba de añadir ahora aparece en la lista del panel **Descripción general**.

El usuario puede ahora activar el evento definido por el usuario manualmente en XProtect Smart Client si el usuario tiene permisos para hacerlo.

> Si elimina un evento definido por el usuario, esto afecta a cualquier regla en la que el evento definido por el usuario esté en uso. Asimismo, un evento eliminado definido por el usuario solo desaparece de XProtect Smart Client cuando el usuario de XProtect Smart Client cierra sesión.

Cambiar nombre de un evento definido por el usuario

> Si cambia el nombre de un evento definido por el usuario, los usuarios de XProtect Smart Client ya conectados deben cerrar sesión y volver a iniciar sesión antes de que el cambio del nombre sea visible.

1. Expandir **Reglas y Eventos** > **Eventos definidos por el usuario**.
2. En el panel **Descripción general**, seleccione el evento definido por el usuario.
3. En el panel **Propiedades**, sobrescriba el nombre existente.
4. En la barra de herramientas, haga clic en **Guardar**.

Añadir y editar un evento de análisis

Añadir un evento de análisis

1. Expanda **Reglas y eventos**, haga clic con el botón derecho en **Eventos de análisis** y seleccione **Añadir nuevo**.
2. En la ventana **Propiedades**, introduzca el nombre del evento en el campo **Nombre**.
3. Introduzca un texto de descripción en el campo **Descripción** en caso necesario.
4. En la barra de herramientas, haga clic en **Guardar**. Pruebe probar la validez del evento haciendo clic en **Pruebas evento**. Continuamente puede corregir los errores indicados en la prueba y ejecutar la prueba tantas veces como quiera y desde cualquier lugar del proceso.

Editar un evento de análisis

1. Haga clic en un evento de análisis existente para ver la ventana **Propiedades**, donde puede editar campos relevantes.
2. Pruebe probar la validez del evento haciendo clic en **Pruebas evento**. Continuamente puede corregir los errores indicados en la prueba y ejecutar la prueba tantas veces como quiera y desde cualquier lugar del proceso.

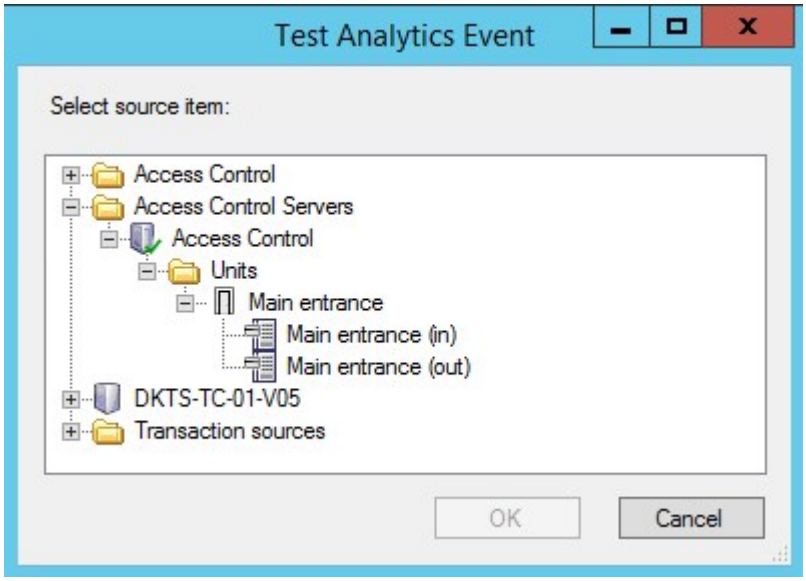
Editar ajustes de eventos de análisis

En la barra de herramientas, vaya a la pestaña **Herramientas** > **Opciones** > **Eventos de análisis** para editar los ajustes relevantes.

Probar un evento de análisis

Después de crear un evento de análisis, puede probar los requisitos (consulte Añadir y editar un evento de análisis en la página 291), por ejemplo que la función de eventos de análisis se ha habilitado en Management Client.

1. Seleccione un evento de análisis existente.
2. En las propiedades, haga clic en el botón **Evento de prueba**. Aparece una ventana que muestra todas las fuentes de eventos posibles.



3. Seleccione la fuente de su evento de prueba, por ejemplo, una cámara. La ventana se cierra y aparece una nueva ventana que para por cuatro condiciones que deben cumplirse para que el evento de análisis funcione.

Como prueba adicional, en XProtect Smart Client puede verificar que el evento de análisis se envió al servidor de eventos. Para hacerlo, abra XProtect Smart Client y vea el evento en la pestaña **Gestor de alarmas**.

Añadir un evento genérico

Puede definir eventos genéricos para ayudar al VMS a reconocer cadenas concretas en paquetes de TCP o UDP de un sistema externo. Basándose en un evento genérico, puede configurar Management Client para desencadenar acciones, por ejemplo para iniciar la grabación o alarmas.

Requisitos
Ha habilitado eventos genéricos y ha especificado los destinos de origen permitidos. Si desea más información, consulte Pestaña Eventos genéricos (opciones) en la página 414.

Para añadir un evento genérico:

1. Expanda **Reglas y eventos**.
2. Haga clic con el botón derecho del ratón en **Eventos genéricos** y seleccione **Añadir nuevo**.
3. Cumplimente la información y las propiedades necesarias. Si desea más información, consulte Eventos genéricos y fuentes de datos (propiedades) en la página 532.
4. (opcional) Para validar que la expresión de búsqueda es válida, introduzca una cadena de búsqueda en el campo **Comprobar si la expresión coincide con la cadena del evento** que se corresponda con los paquetes esperados:
   - **Coincidencia**: la cadena se puede validar respecto a la expresión de búsqueda
   - **Sin coincidencia**: la expresión de búsqueda no es válida. Cambiarlo y volver a intentarlo

En XProtect Smart Client, puede verificar si el servidor de eventos ha recibido sus eventos genéricos. Lo hace en la **Lista de alarmas** de la pestaña **Gestor de alarmas** seleccionando **Eventos**.

Autenticación

Registrar las reclamaciones de un PDI externo

1. En Management Client, seleccione **Herramientas** > **Opciones** y abra la pestaña **IDP externo**.
2. En la sección **IDP externo**, seleccione **Añadir**.
3. En la sección **Reclamaciones registradas**, seleccione **Añadir**.
4. Introduzca la información sobre la reclamación. Si desea más información, consulte Registrar reclamaciones.

Asignar reclamaciones de un IDP externo a cometidos en XProtect

En el sitio del IDP externo, el administrador debe crear reclamaciones compuestas por un nombre y un valor. A continuación, la reclamación se asigna a un cometido en el VMS, y los privilegios del usuario estarán determinados por el cometido.

1. Desde el panel de **Navegación del sitio** en Management Client, despliegue el nodo de **Seguridad** y seleccione **Cometidos**.
2. Seleccione un cometido, seleccione la pestaña **IDP externo** y seleccione **Añadir**.
3. Seleccione un IDP externo y un nombre de reclamación e introduzca un valor de reclamación.

   El nombre de la reclamación debe escribirse exactamente como el nombre de la reclamación que viene del IDP externo.

4. Seleccione **Aceptar**.

Si se elimina un IDP externo, todos los usuarios conectados al VMS mediante el IDP externo también se eliminan. Todas las reclamaciones registradas que están conectadas al IDP externo se quitan y cualquier asignación a cometidos también se elimina.

Inicio de sesión a través de un IDP externo:

Puede iniciar sesión en XProtect Smart Client, XProtect Management Client, XProtect Web Client y en el cliente XProtect Mobile utilizando un IDP externo.

1. En **Autenticación** en el cuadro de diálogo de inicio de sesión en XProtect Smart Client o XProtect Management Client, seleccione el IDP externo y seleccione **Iniciar sesión**. En su primer acceso, será redirigido a una página web perteneciente al IDP externo.
2. Proporcione su nombre de usuario y contraseña e inicie sesión. Una vez que haya iniciado la sesión, volverá al cliente de XProtect y habrá iniciado la sesión.

En **Herramientas** > **Opciones** > **IDP externo**, puede configurar el nombre del IDP externo que se muestra en la lista de **Autenticación**.

Si el IDP externo está deshabilitado, por ejemplo, debido a una restauración o un cambio de contraseña, la opción de iniciar sesión mediante un IDP externo no está disponible en la lista **Autenticación**. Asimismo, si el IDP externo está deshabilitado, el secreto del cliente recibido del IDP externo desaparece del campo **Secreto del cliente** en la pestaña **IDP externo** en **Herramientas** > **Opciones**.

Seguridad

Añadir y gestionar un rol

1. Expanda **Seguridad** y haga clic con el botón derecho en **Roles**.
2. Seleccione **Añadir rol**. Esto abre el cuadro de diálogo **Añadir rol**.
3. Introduzca un nombre y una descripción para el nuevo rol y haga clic en **Aceptar**.
4. El nuevo rol se se añade a a lista **Roles**. De forma predeterminada, un nuevo rol no tiene ningún usuario/grupo asociado, pero tiene una serie de perfiles predeterminados asociados.
5. Para elegir perfiles de Smart Client y Management Client distintos, perfiles de bloqueo de evidencias o perfiles temporales, haga clic en las listas desplegables.
6. Ahora puede asignar usuarios/grupos al rol, y especificar a cuáles de las características del sistema pueden acceder.

Si desea más información, consulte Asignar/eliminar usuarios y grupos a/de roles en la página 296 y Roles (nodo Seguridad) en la página 537.

Copiar, cambiar nombre o eliminar un rol

Copiar un rol

Si tiene un cometido con configuraciones y/o permisos complicados y necesita un cometido similar o casi similar, puede ser más fácil copiar el cometido ya existente y hacer pequeños ajustes en la copia que crear un nuevo cometido desde cero.

1. Expanda **Seguridad**, haga clic en **Roles**, haga clic con el botón derecho en el rol relevante y seleccione **Copiar rol**.
2. En el cuadro de diálogo que se abre, dé al rol copiado un nombre único y una descripción.
3. Haga clic en **Aceptar**.

Cambiar nombre de un rol

Si cambia el nombre de un rol, esto no cambia el nombre del grupo de vistas en función del rol.

1. Expanda **Seguridad** y haga clic con el botón derecho en **Roles**.
2. Haga clic con el botón derecho del ratón en el rol requerido y seleccione **Cambiar nombre de rol**.
3. En el cuadro de diálogo que se abre, cambie el nombre del rol.
4. Haga clic en **Aceptar**.

Eliminar un rol

1. Expanda **Seguridad** y haga clic en **Roles**.
2. Haga clic con el botón derecho del ratón en el rol que no desee y seleccione **Eliminar rol**.
3. Haga clic en **Sí**.

Si elimina un rol, no se elimina el grupo de vistas basado en el rol.

Ver roles efectivos

Con la función Roles efectivos, puede ver todos los roles de un usuario o grupo seleccionado. Esto es práctico si está utilizando grupos y es la única forma de visualizar de qué roles es miembro un usuario específico.

1. Abra la ventana **Roles efectivos** expandiendo **Seguridad**, luego haga clic con el botón derecho en **Roles** y seleccione **Roles efectivos**.
2. Si quiere información sobre un usuario básico, introduzca el nombre en el campo **Nombre de usuario**. Haga clic en **Actualizar** para mostrar los roles funciones de los usuarios.
3. Si utiliza usuarios o grupos de Windows en Active Directory, haga clic en el botón de exploración "**...**". Seleccione el tipo de objeto, introduzca el nombre y haga clic en **Aceptar**. Los roles del usuario aparecen automáticamente.

Asignar/eliminar usuarios y grupos a/de roles

Para asignar o quitar usuarios o grupos de Windows, o usuarios básicos de a/de un rol:

1. Expanda **Seguridad** y seleccione **Roles**. A continuación, seleccione el rol requerido en el panel **Descripción general**:
2. En el panel **Propiedades**, seleccione la pestaña **Usuarios y grupos** en la parte inferior.
3. Haga clic en **Añadir**, seleccione **Usuario de Windows** o **Usuario básico**.

Asignar usuarios de Windows y grupos a un rol

1. Seleccione **Usuario de Windows**. Esto abre el cuadro de diálogo **Seleccionar Usuarios**, **Ordenadores y Grupos**:
2. Verifique que el se ha especificado el tipo de objeto requerido. Si, por ejemplo, necesita añadir un ordenador, haga clic en **Tipos de objeto** y marque **Ordenador**. Verifique también que el dominio requerido está especificado en el campo **Desde esta ubicación**. Si no, haga clic en **Ubicaciones** para explorar el dominio requerido.
3. En el cuadro **Introducir los nombres de objetos que seleccionar**, introduzca los nombres de usuario relevantes, las iniciales u otros tipos de identificador que Active Directory puede reconocer. Utilice la característica **Comprobar nombres** para verificar que Active Directory reconoce los nombres o iniciales que ha introducido. Como alternativa, utilice la función **"Avanzado..."** para buscar usuarios y grupos.

4. Haga clic en **Aceptar**. Los usuarios/grupos seleccionados ahora se añaden a la lista de usuarios de la pestaña **Usuarios y grupos** a los que ha asignado el rol seleccionado. Puede añadir más usuarios y grupos introduciendo múltiples nombres separados por punto y coma (**;**).

Asignar usuarios básicos a un rol

1. Seleccione **Usuario básico**. Esto abre el cuadro de diálogo **Seleccionar usuarios básicos para añadir al rol**:
2. Seleccione a los usuarios básicos que quiera asignar a este rol.
3. Opcional: Haga clic en **Nuevo** para crear un usuario básico nuevo.
4. Haga clic en **Aceptar**. Los usuarios seleccionados ahora se añaden a la lista de usuarios básicos de la pestaña **Usuarios y grupos** a los que ha asignado el rol seleccionado.

Quitar usuarios y grupos de un rol

1. En la pestaña **Usuarios y Grupos**, seleccione el usuario o grupo que quiere quitar y haga clic en **Quitar** en la parte inferior de la pestaña. Puede seleccionar más de un usuario o grupo, o una combinación de grupos y usuarios individuales, si necesita hacerlo.
2. Confirme que quiere eliminar los usuarios y/o grupos seleccionados. Haga clic en **Sí**.

> Un usuario también puede tener roles en los grupos a los que pertenezca. Cuando ese es el caso, no puede quitar al usuario individual del rol. Los miembros del grupo también pueden tener roles como individuos. Para averiguar qué roles tienen los usuarios, grupos o miembros de grupos individuales, utilice la función **Ver roles efectivos**.

Crear usuarios básicos

Existen dos tipos de cuentas de usuario de Milestone XProtect VMS: Usuarios básicos y usuarios de Windows.

Los usuarios básicos son cuentas de usuario que crea en Milestone XProtect VMS. Se trata de una cuenta de usuario del sistema dedicada con un nombre de usuario básico y una contraseña de autenticación para cada usuario individual.

Los usuarios de Windows son cuentas de usuario que añades a través de Active Directory de Microsoft.

Hay algunas diferencias básicas entre usuarios básicos y usuarios de Windows:

- Los usuarios básicos se autentican mediante una combinación de nombre de usuario y contraseña y son específicos de un sitio/sistema. Tenga en cuenta que aunque un usuario básico creado en un sitio federado tenga el mismo nombre y contraseña que un usuario básico de otro sitio federado, el usuario básico solo tiene acceso al sitio en el que se ha creado.
- Los usuarios de Windows se autentifican mediante su inicio de sesión en Windows y son específicos de una máquina.

Configurar los ajustes de inicio de sesión para usuarios básicos

Puede definir la configuración de inicio de sesión para usuarios básicos en un archivo JSON, que se encuentra aquí: `\\Archivos de programa\Milestone\Management Server\IIS\IDP\appsettings.json`.

En ese archivo, puede establecer los siguientes parámetros:

LoginSettings	
"ExpireTimeInMinutes": 5	Defina la duración de tiempo (en minutos) tras el que el inicio de sesión experidará si el usuario no realiza ninguna acción.
LockoutSettings	
"LockoutTimeSpanInMinutes": 5	Defina la duración de tiempo (en minutos) tras el que el usuario será bloqueado.
"MaxFailedAccessAttempts": 5	Defina el número de intentos que tendrá un usuario para iniciar sesión antes de ser bloqueado.
PasswordSettings	
"RequireDigit": true	Defina si en la contraseña debe contener dígitos básicos (de 0 a 9).
"RequireLowercase": true	Defina si la contraseña debe contener caracteres en minúscula.
"RequireNonAlphanumeric": true	Defina si la contraseña debe contener caracteres especiales (~!@#$%^&*_-+=|\(){}[]:;"'<>,.?/).
"RequireUppercase": true	Defina si la contraseña debe contener caracteres en mayúscula.
"RequiredLength": 8	Defina el número de caracteres que debe tener la contraseña. Hay una longitud mínima para la contraseña de {0} caracteres y una longitud máxima para la contraseña de 255 caracteres.
"RequiredUniqueChars": 1	Defina el número mínimo de caracteres únicos obligatorios en una contraseña. Por ejemplo, si establecer el número de caracteres únicos requeridos en 2, entonces contraseñas como "aaaaaa, aa, a, b, bb, bbbbbbb" serán rechazadas.

	Mientras que, abab, abc, aaab, etc., se aceptarán porque hay al menos dos caracteres únicos en la contraseña. Aumentar el número de caracteres únicos en una contraseña, aumenta la fortaleza de la contraseña evitando secuencias repetitivas que son fáciles de adivinar.

Para crear un usuario básico en su sistema:

1. Expanda **Seguridad** > **Usuarios básicos**.
2. En el panel **Usuarios básicos**, haga clic con el botón derecho y seleccione **Crear usuario básico**.
3. Especifique un nombre de usuario y una contraseña. Repita la contraseña para asegurarse de que la ha especificado correctamente.

   La contraseña debe cumplir la complejidad definida en el archivo **appsettings.json** (consulte Configurar los ajustes de inicio de sesión para usuarios básicos en la página 298).
4. Especifique si el usuario básico debe debe cambiar la contraseña en el siguiente inicio de sesión. Milestone recomienda activar la casilla de verificación para que los usuarios básicos puedan especificar sus propias contraseñas cuando inicien sesión por primera vez.

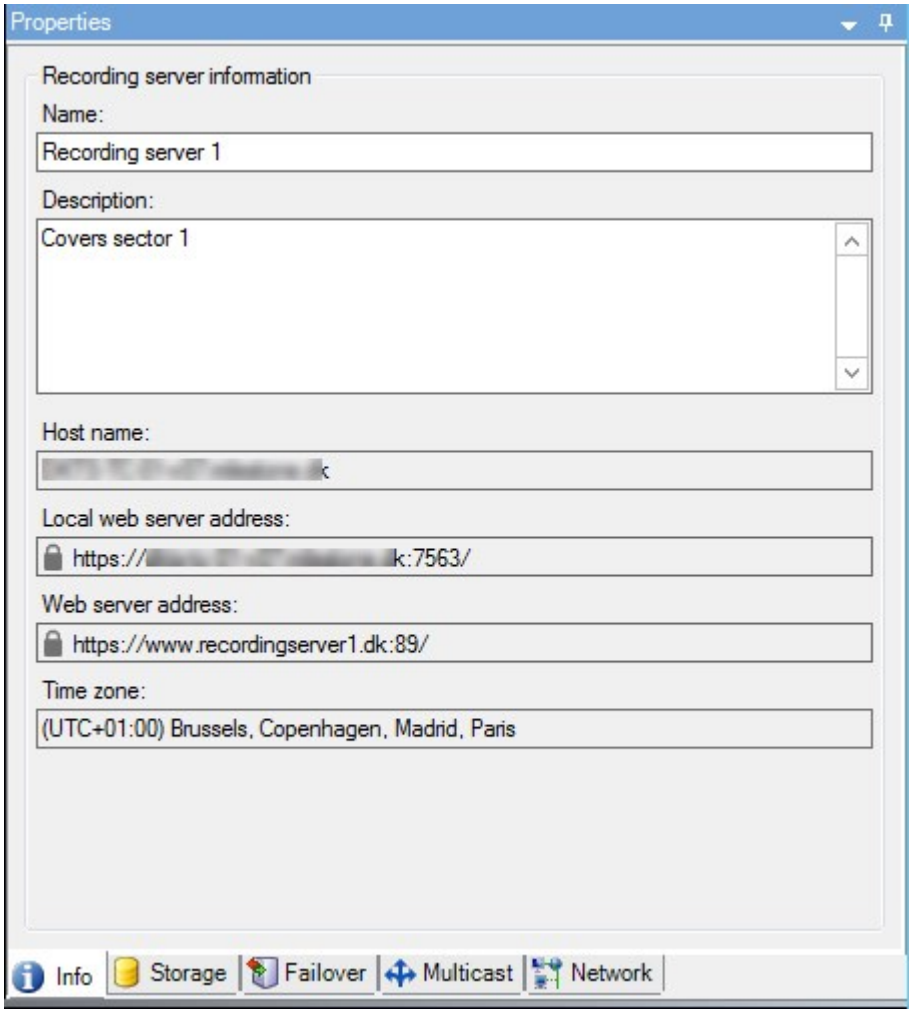
   Debe desactivar la casilla de verificación únicamente al crear usuarios básicos que no puedan cambiar su contraseña. Estos usuarios básicos son, por ejemplo, usuarios del sistema utilizados para plug-ins y autenticación de servicios del servidor.
5. Especifique el estado del usuario básico para que sea **Habilitado** o **Bloqueado**.
6. Haga clic en **Aceptar** para crear el usuario básico.

Ver el estado del cifrado a los clientes

Para verificar si su servidor de grabación cifra las conexiones:

1. Abra el Management Client.
2. En el panel de **Navegación del sitio**, seleccione **Servidores** > **Servidores de grabación**. Esto abre una lista de servidores de grabación.

3. En el panel **Generalidades**, seleccione el servidor de grabación correspondiente y vaya a la pestaña de **Información**.
   Si se habilita el cifrado a los clientes y servidores que recuperan flujos de datos del servidor de grabación, aparecerá un icono de un candado delante de la dirección del servidor web local y de la dirección del servidor web opcional.



Panel del sistema

Ver tareas en curso actualmente en servidores de grabación

La ventana **Tareas actuales** muestra una descripción general de tareas en curso en un servidor de grabación seleccionado. Si ha iniciado una tarea que tarda mucho tiempo y se ejecuta en segundo plano, puede abrir la ventana **Tareas actuales** para ver cómo progresa la tarea. Unos pocos ejemplos de tareas de larga duración iniciadas por el usuario son actualizaciones de firmware y movimiento de hardware. Puede ver información sobre la hora de inicio de las tareas, la hora de finalización estimada y el progreso.

Si la tarea no progresa según lo esperado, probablemente puede encontrar la causa en el hardware o en la red. Unos pocos ejemplos son que el servidor no está en funcionamiento, error del servidor, ancho de banda demasiado pequeño pérdida de conexión.

1. En el panel **Navegación por el sitio**, seleccione el **Panel de control del sistema** > **Tareas actuales**.
2. Seleccione un servidor de grabación para ver sus tareas actuales.

La información que se muestra en la ventana **Tareas actuales** no se actualiza de forma dinámica, sino que es una instantánea de las tareas actuales desde el momento en que abrió la ventana. Si ha tenido abierta la ventana durante algún tiempo, actualice la información seleccionando el botón **Actualizar** en la esquina inferior derecha de la ventana.

Monitor del sistema (explicación)

La funcionalidad del monitor del sistema requiere que el servicio Data Collector esté en ejecución y solo funciona en ordenadores que utilizan un calendario gregoriano (Occidente).

Panel de control del monitor del sistema (explicación)

En el **Panel de control del monitor del sistema**, puede obtener fácilmente una descripción general del estado de su sistema VMS. El estado de su hardware se representa visualmente por mosaicos y sus colores: verde (en ejecución), amarillo (advertencia) y rojo (crítico). Los archivos también pueden tener iconos de error o advertencia cuando uno o más componentes de hardware presentan un estado defectuoso.

De forma predeterminada, el sistema muestra mosaicos que representan todos los **Servidores de grabación**, **Todos los servidores** y **Todas las cámaras**. Puede personalizar los parámetros de monitorización de estos mosaicos predeterminados y crear mosaicos nuevos. Por ejemplo, puede configurar mosaicos para representar un único servidor, una única cámara, un grupo de cámaras o un grupo de servidores.

Los parámetros de monitorización son, por ejemplo, uso de la CPU o memoria disponible para un servidor. Un mosaico solo monitoriza los parámetros de monitorización que ha añadido al archivo. Consulte Añadir un nuevo mosaico de servidores o cámaras al panel de control del monitor del sistema en la página 304, Editar un mosaico de cámaras o servidores en el panel de control del monitor del sistema en la página 304 y Eliminar un mosaico de cámaras o servidores en el panel de control del monitor del sistema en la página 305 para obtener más información.

Umbrales del monitor del sistema (explicación)

Los umbrales del monitor del sistema le permite definir y ajustar los umbrales cuando los mosaicos en el **Panel de control del monitor del sistema** debe indicar visualmente que el hardware de su sistema cambia de estado. Por ejemplo, cuando el uso de la CPI de un servidor cambia de un estado normal (verde) a un estado de advertencia (amarillo) o de un estado de advertencia (amarillo) a un estado crítico (rojo).

El sistema tiene valores umbrales predeterminados para todo el hardware de este mismo tipo, para que pueda empezar a monitorizar el estado del hardware de su sistema desde el momento en que el sistema esté instalado y haya añadido hardware. También puede configurar valores de umbrales para servidores, cámaras, discos y almacenamientos individuales. Para cambiar los valores de los umbrales, consulte Editar umbrales para cuando los estados del hardware deben cambiar en la página 305.

Para garantizar que no ve un estado **Crítico** o de **Advertencia** en casos en los que el uso o la carga del hardware del sistema alcanza un valor de umbral alto durante un segundo o similar, utilice **Intervalo de cálculo**. Con el ajuste del intervalo de cálculo correcto, no recibirá falsos positivos de alertas sobre umbrales excedidos, sino solo alertas sobre problemas sostenidos con, por ejemplo, el uso de la CPU o el consumo de memoria.

También puede configurar reglas (consulte Reglas (explicación)) para realizar acciones específicas o activar alarmas cuando un umbral cambia de un estado a otro.

Ver el estado actual de su hardware y solucionar problema en caso necesario

En el **Panel de control del monitor del sistema**, puede obtener fácilmente una descripción general del estado de su sistema VMS. El estado de su hardware se representa visualmente por mosaicos y sus colores: verde (en ejecución), amarillo (advertencia) y rojo (crítico). Los archivos también pueden tener iconos de error o advertencia cuando uno o más componentes de hardware presentan un estado defectuoso.

Puede editar los umbrales para cuando el hardware esté en uno de los tres estados. Si desea más información, consulte Editar umbrales para cuando los estados del hardware deben cambiar en la página 305.

El **Panel de control del monitor del sistema** responde a preguntas como: ¿Se están ejecutando todas las cámaras y los servicios del servidor? ¿Son suficientes el uso de la CPI y la memoria disponible en los distintos servidores para que todo se grabe y esté disponible para su visualización?

1. En el panel **Navegación por el sistema**, seleccione **Panel de control del sistema** > **Monitor del sistema**.
2. Si todos los mosaicos están en verde y no hay iconos de advertencia o error, todos los parámetros de monitorización y todos los servidores y cámaras representados por los mosaicos están bien y funcionando.
   Si uno o varios de los mosaicos tienen un icono de advertencia o error, o están totalmente en amarillo o en rojo, seleccione uno de esos mosaicos para solucionar el problema.
3. En la lista de hardware con parámetros de monitorización (parte inferior de la ventana), encuentre el hardware que no se está ejecutando. Coloque el ratón sobre el signo de la cruz roja junto al hardware para leer cuál es el problema.
4. Opcionalmente, seleccione **Detalles** en el lado derecho del hardware para ver cuánto tiempo lleva el problema. Habilite las recopilaciones de datos históricos para ver el estado de su hardware con el tiempo. Si desea más información, consulte Recopilar datos históricos de los estados del hardware en la página 303.
5. Encuentre una forma de solucionar el problema. Por ejemplo, reinicio del ordenador, reinicio servicio del servidor, sustitución de un elemento de hardware defectuoso u otro.

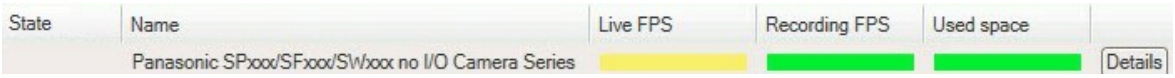
Ver el estado histórico de su hardware e imprimir un informe

Con la característica **Monitor del sistema**, puede obtener fácilmente una descripción genral del estado de su sistema VMS. Asimismo, durante un periodo de tiempo más amplio.

¿Hay periodos en los que el uso de la CPU, el ancho de banda u otro hardware se vean comprometidos? Encuentre la respuesta a esto en la funcionalidad del Monitor del sistema y decida si necesita actualizar el hardware o comprar nuevo para evitarlo en el futuro.

Recuerde habilitar la recopilación de datos históricos. Consulte Recopilar datos históricos de los estados del hardware en la página 303.

1. En el panel **Navegación por el sistema**, seleccione **Panel de control del sistema** > **Monitor del sistema**.
2. En la ventana **Monitor del sistema**, seleccione un mosaico con el hardware del que quiere conocer los datos históricos sobre su estado, o en la parte inferior de la pantalla, seleccione un servidor o una cámara.
3. Seleccione **Detalles** en el lado derecho del servidor o la cámara relevantes.



4. Para servidores, seleccione **Historial** a la derecha del hardware que quiera investigar. Para las cámaras, seleccione el enlace.
5. Si quiere imprimir un informe, seleccione el icono PDF.

Solo puede crear informes históricos con datos del servidor de grabación en el que está actualmente ubicado el dispositivo.

Si accede a los detalles del monitor del sistema desde el sistema operativo de un servidor, puede recibir un mensaje sobre **Configuración de seguridad mejorada de Internet Explorer**. Siga las instrucciones para añadir la página **Monitor del sistema** a la **Zona de sitios de confianza** antes de proceder.

Recopilar datos históricos de los estados del hardware

Puede habilitar la recopilación de datos históricos en el hardware del sistema para ver gráficos de los estados del hardware en el tiempo e imprimir un informe. Si desea más información, consulte Ver el estado histórico de su hardware e imprimir un informe en la página 303.

1. En el panel **Navegación por el sistema**, seleccione **Panel de control del sistema** > **Monitor del sistema**.
2. En la ventana **Monitor del sistema**, seleccione **Personalizar**.

3. En la ventana **Personalizar panel de control** que se abre, seleccione **Recopilar datos históricos**.
4. Seleccione un intervalo de muestreo. Cuanto más corto sea el intervalo, mayor será la carga en la base de datos de SQL Server, el ancho de banda u otro hardware. El intervalo de muestreo de datos históricos también determina el grado de detalle de los gráficos.

Añadir un nuevo mosaico de servidores o cámaras al panel de control del monitor del sistema

Si quiere monitorizar sus cámaras o servidores en grupos más pequeños por su ubicación física, o si quiere monitorizar algún elemento de hardware con distintos parámetros de monitorización, puede añadir mosaicos adicionales a la ventana **Monitor del sistema**.

1. En el panel **Navegación por el sistema**, seleccione **Panel de control del sistema** > **Monitor del sistema**.
2. Enla ventana **Monitor del sistema**, seleccione **Personalizar**.
3. En la ventana **Personalizar panel de control** que se abre, seleccione **Nuevo** en **Mosaicos de servidores** o **Mosaicos de ventanas**.
4. En la ventana **Nuevo mosaico de servidores/Nuevo mosaico de cámaras**, seleccione las cámaras o los servidores que se deben monitorizar.
5. En **Parámetros de monitorización**, seleccione o desactive la selección de las casillas de verificación para cualquier parámetro que quiera añador o quitar del mosaico.
6. Seleccione **Aceptar**. El nuevo mosaico de servidores o cámaras ahora se se añade a los mosaicos que se muestran en el panel de control.

Editar un mosaico de cámaras o servidores en el panel de control del monitor del sistema

Si quiere monitorizar sus cámaras o servidores con otros parámetros de monitorización, puede ajustarlos.

1. En el panel **Navegación por el sistema**, seleccione **Panel de control del sistema** > **Monitor del sistema**.
2. En la ventana **Monitor del sistema**, seleccione **Personalizar**.
3. En la ventana **Personalizar panel de control** que se abre, seleccione el mosaico que quiere cambiar en **Mosaicos de servidores** o **Mosaicos de cámaras** y seleccione **Editar**.
4. En la ventana **Editar mosaico de servidores/cámaras del panel de control**, seleccione todas las cámaras o servidores, un grupo de cámaras o servidores o bien cámaras o servidores individuales para cambiar sus parámetros de monitorización.
5. En **Parámetros de monitorización**, seleccione los parámetros de monitorización que quiera monitorizar.
6. Seleccione **Aceptar**.

Eliminar un mosaico de cámaras o servidores en el panel de control del monitor del sistema

Si ya no necesita monitorizar el hardware representado por un mosaico, puede eliminar el mosaico.

1. En el panel **Navegación por el sistema**, seleccione **Panel de control del sistema** > **Monitor del sistema**.
2. Enla ventana **Monitor del sistema**, seleccione **Personalizar**.
3. En la ventana **Personalizar panel de control** que se abre, seleccione el mosaico que quiere cambiar en **Mosaicos de servidores** o **Mosaicos de cámaras**.
4. Seleccione **Eliminar**.

Editar umbrales para cuando los estados del hardware deben cambiar

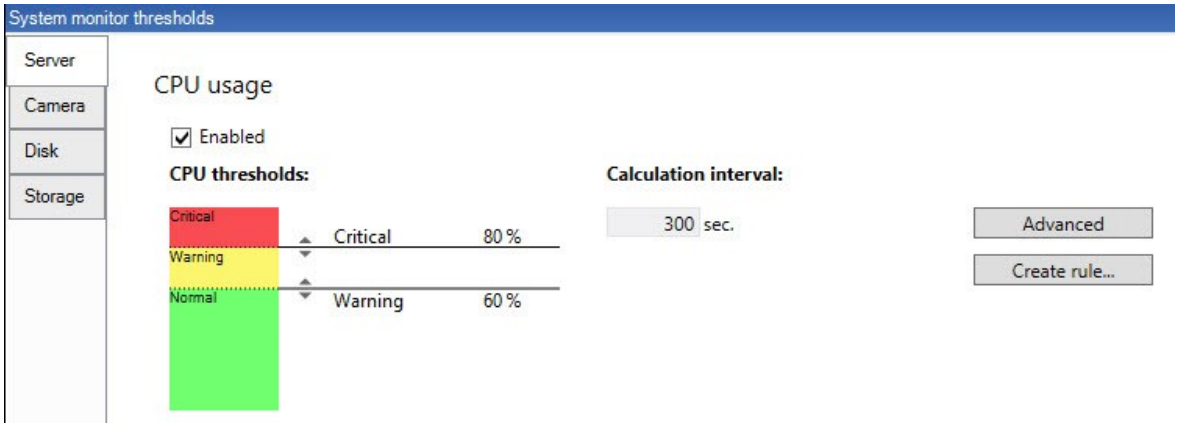
Puede editar los umbrales para cuando el hardware cambie entre los tres estados en el **Panel de control del monitor del sistema**. Si desea más información, consulte Umbrales del monitor del sistema (explicación) en la página 301.

Puede cambiar umbrales para distintos tipos de hardware. Si desea más información, consulte Umbrales del monitor del sistema (nodo Panel del sistema) en la página 597.

De forma predeterminada, el sistema está configurado para mostrar valores umbrales para todas las unidades del mismo tipo de hardware, por ejemplo, todas las cámaras o servidores. Puede cambiar estos valores de umbrales predeterminados.

También puede configurar valores de umbrales para cámaras o servidores individuales o para un subconjunto de estos con el fin de permitir, por ejemplo, que algunas cámaras utilicen valores más altos de **FPS en directo** o **FPS de grabación** que otras cámaras.

1. En el panel **Navegación por el sitio**, seleccione **Panel de control del sistema** > **Umbrales del monitor del sistema**.
2. Seleccione la casilla de verificación **Habilitado** para el hardware relevante si aún no lo ha habilitado. La figura siguiente muestra un ejemplo.



3. Arrastre el control deslizante del control del umbral arriba o abajo para aumentar o disminuir el valor del umbral. Hay dos controles deslizantes disponibles para cada componente de hardware mostrado en el control del umbral, que separan los estados **Normal**, **Advertencia** y **Crítico**.
4. Introduzca un valor para el intervalo de cálculo o conserve el valor predeterminado.
5. Si quiere establecer valores en elementos individuales de hardware, seleccione **Avanzados**.
6. Si quiere especificar reglas para determinados eventos o dentro de intervalos de tiempo específicos, seleccione **Crear regla**.
7. Una vez establecidos los niveles de los umbrales y los intervalos de cálculo, seleccione **Archivo** > **Guardar** en el menú.

Ver bloqueos de evidencias en el sistema

Bloqueo de evidencias en el nodo **Panel de control del sistema** muestra una descripción general de todos los datos protegidos en el sistema de vigilancia actual.

Encuentre un bloqueo de evidencia filtrando después, por ejemplo, quién lo creó o cuándo.

1. En el panel **Navegación por el sitio**, seleccione **Panel de control del sistema** > **Bloqueo de evidencias**.
2. Obtenga una descripción general y encuentre los bloqueos de evidencias relevantes. Puede filtrar después y ordenar los distintos metadatos relacionados con los bloqueos de evidencias.

Toda la información que se muestra en la ventana **Bloqueo de evidencias** son instantáneas. Pulse F5 para actualizar.

Imprimir un informe con la configuración del sistema

Al instalar y configurar el sistema VMS, se hacen muchas elecciones y es posible que tenga que documentarlas. Con el tiempo también es difícil recordar todos los ajustes que se han cambiado desde la instalación y la configuración inicial, o solo durante el último par de meses. Por este motivo es posible imprimir un informe con todas sus opciones de configuración.

Al crear un informe de configuración (formato PDF), puede añadir cualquier posible elemento de su sistema al informe. Puede, por ejemplo, incluir licencias, configuración de dispositivos, configuración de alarmas y mucho más. Puede seleccionar la opción **Excluir datos sensibles** para crear un informe que cumpla el RGPD (habilitado de forma predeterminada). También puede personalizar la fuente, la configuración de la página y la portada.

1. Expanda **Panel de control del sistema** y seleccione **Informes de configuración**.
2. Seleccione los elementos que quiere incluir o excluir en su informe.
3. **Opcional**: Si ha seleccionado incluir una portada, seleccione **Portada** para personalizar la información en su portada. En la ventana que aparece, cumplimente la información necesaria.
4. Seleccione **Formato** para personalizar la fuente, el tamaño de la página y los márgenes. En la ventana que aparece, seleccione los ajustes deseados.
5. Cuando esté listo para exportar, seleccione **Exportar** y seleccione un nombre y una ubicación de guardado para su informe.

Solo los usuarios con permisos de administrador en el sistema VMS pueden crear informes de configuración.

Metadatos

Mostrar u ocultar categorías de búsqueda de metadatos y filtros de búsqueda

Los usuarios de XProtect Management Client con permisos de administrador pueden mostrar u ocultar las categorías de búsqueda de metadatos por defecto Milestone y los filtros de búsqueda en XProtect Smart Client. De forma predeterminada, estas categorías de búsqueda y estos filtros de búsqueda están ocultos. Mostrarlos es útil si el sistema de videovigilancia cumple los requisitos (consulte Requisitos de la búsqueda de metadatos en la página 604).

Este ajuste afecta a todos los usuarios de XProtect Smart Client.

Este ajuste no afecta a la visibilidad de:

- Otras categorías de búsqueda y filtros de búsqueda que no son metadatos Milestone, por ejemplo **Movimiento**, **Marcadores**, **Alarmas** y **Eventos**
- Categorías de búsqueda de terceros y filtros de búsqueda

1. En XProtect Management Client, en el panel **Navegación en sitio**, seleccione **Uso de metadatos** > **Búsqueda de metadatos**.
2. En el panel **Búsqueda de metadatos**, seleccione la categoría de búsqueda para la que quiere cambiar los ajustes de visibilidad.
3. Para habilitar la visibilidad de una categoría de búsqueda o un filtro de búsqueda, seleccione la casilla de verificación correspondiente. Para deshabilitar la visibilidad de una categoría de búsqueda o un filtro de búsqueda, desactive la casilla de verificación.

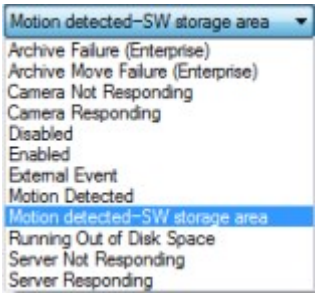
Alarmas

Añadir una alarma

Para definir una alarma, es necesario crear una definición de alarma, en la que se especifica, por ejemplo, qué es lo que activa la alarma, las instrucciones sobre lo que debe hacer el operador y qué o cuándo se detiene la alarma. Para obtener información detallada sobre los ajustes, consulte Definiciones de alarmas (nodo Alarmas).

1. En el panel de **Navegación del sitio**, expanda **Alarmas**, y haga clic con el botón derecho en **Definiciones de alarma**.
2. Seleccione **Añadir nuevo**.

3. Rellene estas propiedades:
    - **Nombre**: Introduzca un nombre para la definición de la alarma. El nombre de la definición de la alarma aparece siempre que la definición de la alarma aparece en la lista.
    - **Instrucciones**: Puede escribir instrucciones para el operador que recibe la alarma.
    - **Evento activador**: Utilice los menús desplegables para seleccionar un tipo de evento y un mensaje de evento que se utilizará cuando se active la alarma.

      Una lista de eventos de activación seleccionables. La que se destaca se crea y personaliza utilizando eventos de análisis.
    - **Fuentes**: Seleccione las cámaras u otros dispositivos de los que debe provenir el evento para activar la alarma. Sus opciones dependen del tipo de evento que haya seleccionado.
    - **Perfil temporal**: Si desea que la alarma se active durante un intervalo de tiempo específico, seleccione el botón de radio y luego un perfil temporal en el menú desplegable.
    - **Basado en eventos**: Si desea que la definición de alarma se active mediante un evento, seleccione el botón de opción y especifique el evento que activará la definición de alarma. También debe especificar un evento que desactivará la definición de alarma.
4. En el menú desplegable **Límite de tiempo**, especifique un límite de tiempo para cuando la acción sea requerida por el operador.
5. En el menú desplegable **Eventos activados**, especifique qué evento debe activarse cuando haya pasado el límite de tiempo.
6. Especifique los ajustes adicionales, por ejemplo, las cámaras relacionadas y el propietario de la alarma inicial.

Habilitar cifrado

Habilitar encriptación en y desde el servidor de gestión

Puede cifrar la conexión bidireccional entre el servidor de gestión y el Data Collector afiliado cuando tiene un servidor remoto del siguiente tipo:

- Recording Server
- Event Server
- Log Server
- LPR Server
- Mobile Server

Si su sistema contiene varios servidores de grabación o servidores remotos, debe habilitar el cifrado en todos ellos.

> Al configurar la encriptación para un grupo de servidores, debe habilitarse con un certificado perteneciente al mismo certificado de la AC o, si la encriptación está deshabilitada, entonces se debe deshabilitar en todos los ordenadores del grupo de servidores.

Requisitos previos:

- Se confía en un certificado de autentificación del servidor en el ordenador que aloja el servidor de gestión

En primer lugar, habilite el cifrado en el servidor de gestión.

Pasos:

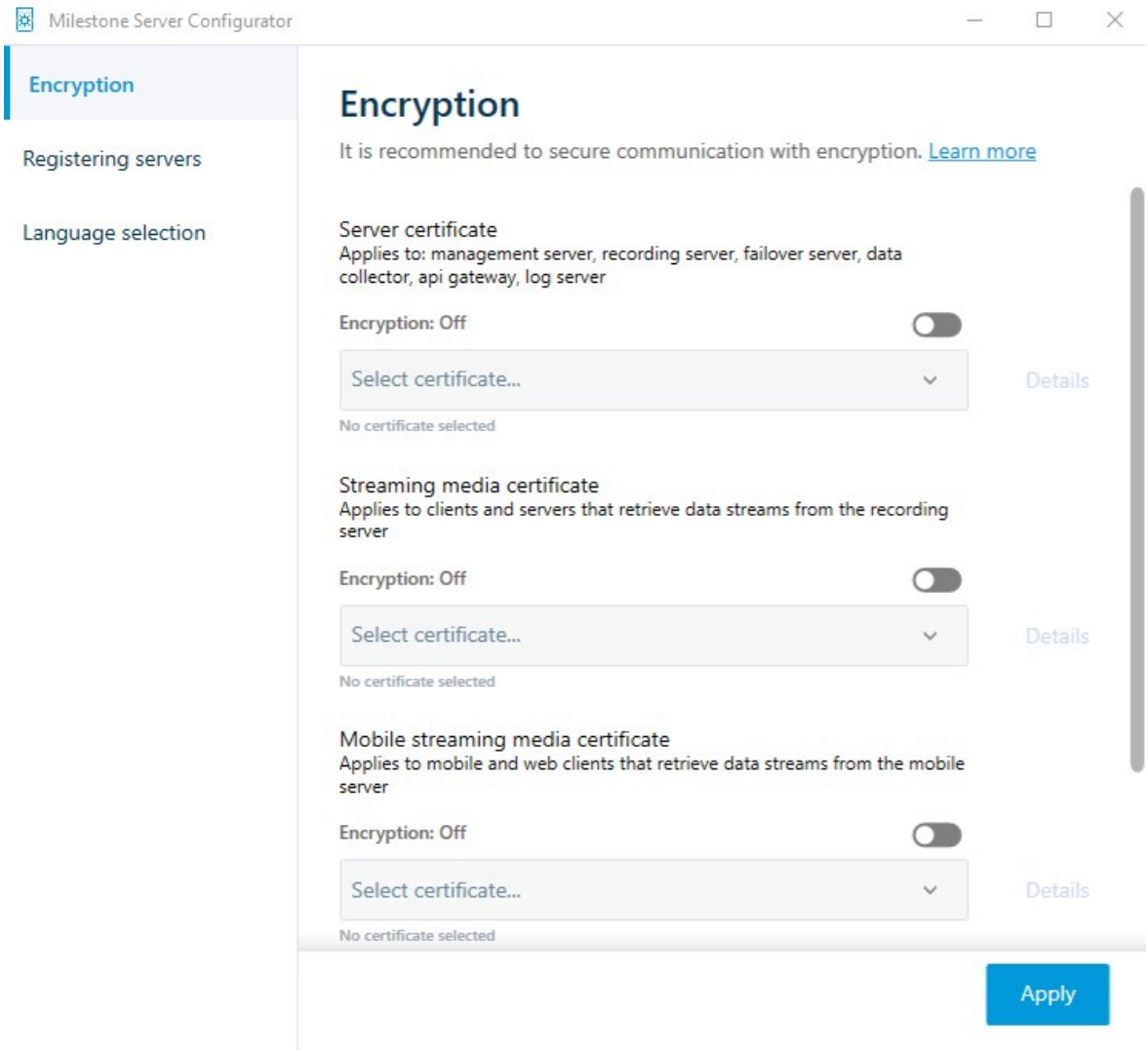
1. En un ordenador con un servidor de gestión instalado, abra el **Server Configurator** de:
   - El menú Inicio de Windows

   o

   - El Management Server Manager haciendo clic con el botón derecho en el icono Management Server Manager de la barra de tareas del ordenador
2. En el **Server Configurator**, en **Certificado de servidor**, encienda **Cifrado**.
3. Haga clic en **Seleccionar certificado** para abrir una lista con nombres de asunto únicos de certificados que tienen una clave privada y que están instalados en el ordenador local en el almacén de certificados de Windows.
4. Seleccione un certificado para cifrar la comunicación entre el servidor de grabación, el servidor de gestión, el servidor failover y el Data Collector server.

   Seleccione **Detalles** para ver la información del almacenamiento de certificados de Windows sobre el

certificado seleccionado.



5.

6. Haga clic en **Aplicar**.

Para completar la habilitación del cifrado, el siguiente paso es actualizar los ajustes del cifrado en cada servidor de grabación y en cada servidor con Data Collector (Event Server, Log Server, LPR Server, y Mobile Server).

Si desea más información, consulte Habilitar encriptación del servidor para servidores de grabación o servidores remotos en la página 311.

Habilitar encriptación del servidor para servidores de grabación o servidores remotos

Puede cifrar la conexión de dos direcciones entre el servidor de gestión y el de grabación u otros servidores remotos que utilizan el Data Collector.

Si su sistema contiene varios servidores de grabación o servidores remotos, debe habilitar el cifrado en todos ellos.

Si desea más información, consulte la guía de certificados sobre cómo asegurar sus instalaciones XProtect VMS.

> Al configurar la encriptación para un grupo de servidores, debe habilitarse con un certificado perteneciente al mismo certificado de la AC o, si la encriptación está deshabilitada, entonces se debe deshabilitar en todos los ordenadores del grupo de servidores.

Requisitos previos:

- Ha habilitado la encriptación en el servidor de gestión, consulte Habilitar encriptación en y desde el servidor de gestión en la página 309.

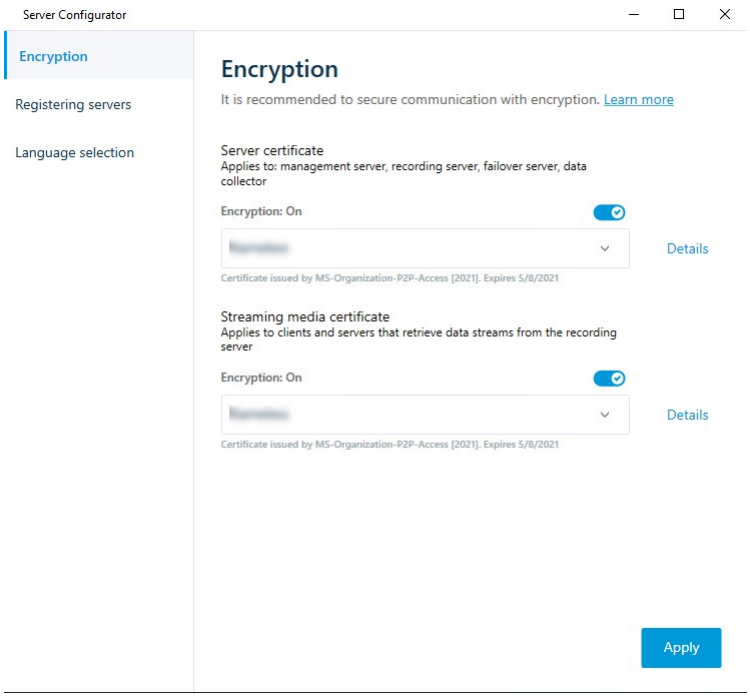
1. En un ordenador con un Management Server o Recording Server instalado, abra el **Server Configurator** desde:
   - El menú Inicio de Windows

   o

   - El gestor de servidor, haciendo clic con el botón derecho en el icono del gestor de servidor en la barra de tareas del ordenador
2. En el **Server Configurator**, en **Certificado de servidor**, encienda **Cifrado**.
3. Haga clic en **Seleccionar certificado** para abrir una lista con nombres de asunto únicos de certificados que tienen una clave privada y que están instalados en el ordenador local en el almacén de certificados de Windows.
4. Seleccione un certificado para cifrar la comunicación entre el servidor de grabación, el servidor de gestión, el servidor de failover y el servidor de recogida de datos.

   Seleccione **Detalles** para ver la información del almacenamiento de certificados de Windows sobre el certificado. seleccionado.

   El usuario del servicio Recording Server ha recibido acceso a la clave privada. Es necesario que este certificado sea de confianza en todos los clientes.



5. Haga clic en **Aplicar**.

Cuando aplique los certificados, el servidor de grabación se detendrá y se reiniciará. Detener el servicio Recording Server significa que no se puede grabar ni ver vídeo en directo mientras se verifica o cambia la configuración básica del servidor de grabación.

Habilitar el cifrado del servidor de eventos

Puede cifrar la conexión bidireccional entre el servidor de eventos y los componentes que se comunican con el servidor de eventos, incluyendo el LPR Server.

Al configurar la encriptación para un grupo de servidores, debe habilitarse con un certificado perteneciente al mismo certificado de la AC o, si la encriptación está deshabilitada, entonces se debe deshabilitar en todos los ordenadores del grupo de servidores.

Requisitos previos:

- Un certificado de autentificación del servidor es de confianza en el ordenador que alberga el servidor de eventos

En primer lugar, habilite el cifrado en el servidor de eventos.

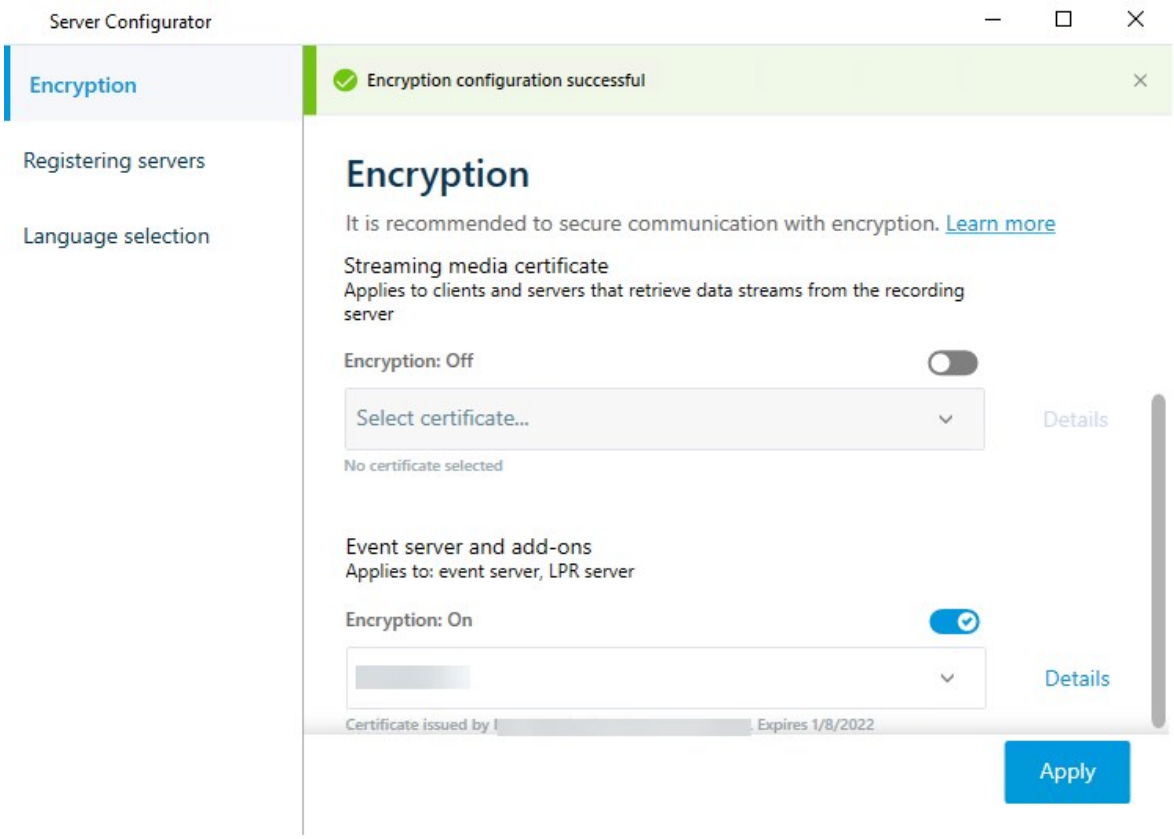
Pasos:

1. En un ordenador con un servidor de eventos instalado, abra el **Server Configurator** de:
   - El menú Inicio de Windows

   o

   - El Event Server haciendo clic con el botón derecho en el icono Event Server de la barra de tareas del ordenador
2. En el **Server Configurator**, en **Servidor de eventos y add-ons**, encienda **Cifrados**.
3. Haga clic en **Seleccionar certificado** para abrir una lista con nombres de asunto únicos de certificados que tienen una clave privada y que están instalados en el ordenador local en el almacén de certificados de Windows.
4. Seleccione un certificado para cifrar la comunicación entre el servidor de eventos y los complementos relacionados.

   Seleccione **Detalles** para ver la información del almacenamiento de certificados de Windows sobre el certificado seleccionado.



5. Haga clic en **Aplicar**.

Para completar la habilitación del cifrado, el siguiente paso es actualizar la configuración del cifrado en cada add-on relacionado LPR Server .

Habilitar encriptación en clientes y servidores

Puede cifrar las conexiones desde el servidor de grabación a los clientes y servidores que transmiten datos desde el servidor de grabación.

> Al configurar la encriptación para un grupo de servidores, debe habilitarse con un certificado perteneciente al mismo certificado de la AC o, si la encriptación está deshabilitada, entonces se debe deshabilitar en todos los ordenadores del grupo de servidores.

Requisitos previos:

- El certificado de autentificación del servidor a utilizar es de confianza en todos los ordenadores que ejecutan servicios que recuperan flujos de datos del servidor de grabación
- XProtect Smart Client y todos los servicios que recuperan flujos de datos del servidor de grabación deben ser de la versión 2019 R1 o posterior
- Es posible que haya que actualizar algunas soluciones de terceros creadas con versiones de MIP SDK anteriores a 2019 R1

Pasos:

1. En un ordenador con un servidor de grabación instalado, abra el **Server Configurator** desde:
   - El menú Inicio de Windows

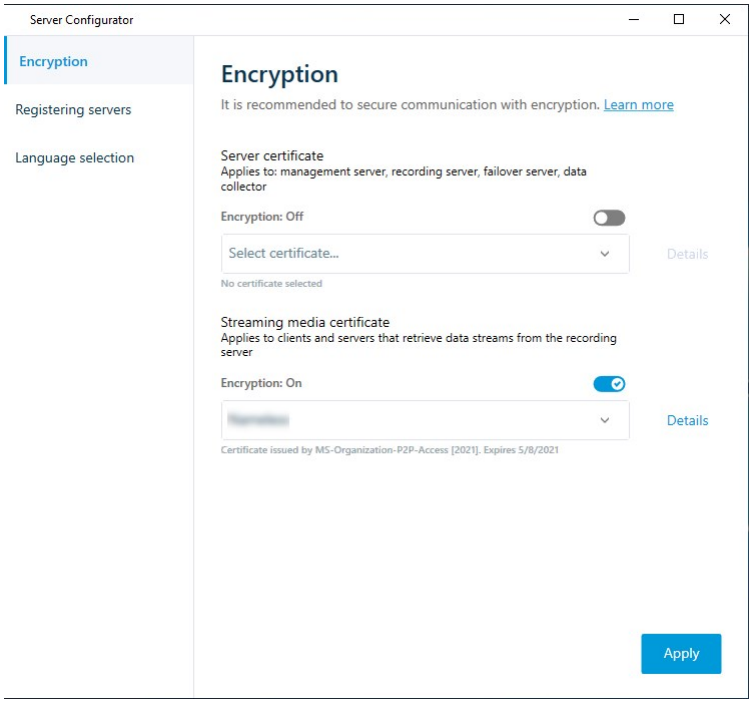
   o

   - El Recording Server Manager haciendo clic con el botón derecho en el icono Recording Server Manager de la barra de tareas del ordenador
2. En el **Server Configurator**, en **Certificado de medios de transmisión**, encienda **Cifrado**.
3. Haga clic en **Seleccionar certificado** para abrir una lista con nombres de asunto únicos de certificados que tienen una clave privada y que están instalados en el ordenador local en el almacén de certificados de Windows.
4. Seleccione un certificado para cifrar la comunicación entre los clientes y los servidores que recuperan los flujos de datos del servidor de grabación.

   Seleccione **Detalles** para ver la información del almacenamiento de certificados de Windows sobre el certificado seleccionado.

   El usuario del servicio Recording Server ha recibido acceso a la clave privada. Es necesario que este

certificado sea de confianza en todos los clientes.



5. Haga clic en **Aplicar**.

> Cuando aplique los certificados, el servidor de grabación se detendrá y se reiniciará. Detener el servicio Recording Server significa que no se puede grabar ni ver vídeo en directo mientras se verifica o cambia la configuración básica del servidor de grabación.

Para verificar si el servidor de grabación utiliza el cifrado, consulte Ver el estado del cifrado para los clientes.

Habilitar encriptación en el servidor móvil

Para usar un protocolo HTTPS con el fin de establecer una conexión segura entre el servidor móvil y los clientes y servicios, debe aplicar un certificado válido en el servidor. El certificado confirma que el titular del certificado está autorizado a establecer conexiones seguras.

Si desea más información, consulte la guía de certificados sobre cómo asegurar sus instalaciones XProtect VMS.

> Al configurar la encriptación para un grupo de servidores, debe habilitarse con un certificado perteneciente al mismo certificado de la AC o, si la encriptación está deshabilitada, entonces se debe deshabilitar en todos los ordenadores del grupo de servidores.

Los certificados emitidos por la AC (Autoridad Certificadora) tienen una cadena de certificados y en la raíz de esa cadena está el certificado raíz de la AC. Cuando un dispositivo o navegador ve este certificado, compara su certificado raíz con los preinstalados en el SO (Android, iOS, Windows, etc.). Si el certificado raíz está recogido en la lista de certificados preinstalados, entonces el SO garantiza al usuario que la conexión con el servidor es lo bastante segura. Estos certificados se emiten para un nombre de dominio y no son gratuitos.

Pasos:

1. En un ordenador con un servidor móvil instalado, abra el **Server Configurator** desde:
   - El menú Inicio de Windows

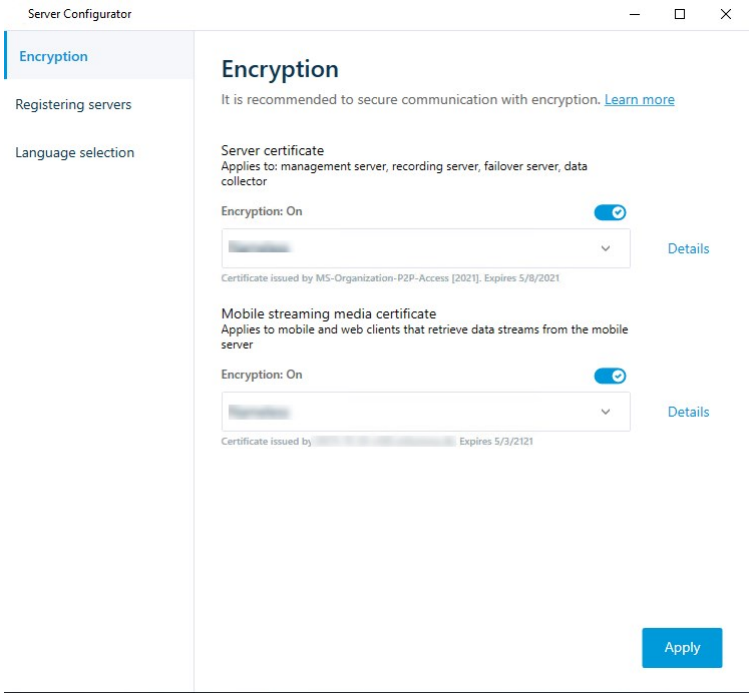
   o

   - El Mobile Server Manager haciendo clic con el botón derecho en el icono Mobile Server Manager de la barra de tareas del ordenador
2. En el **Server Configurator**, bajo **Certificado de medios de transmisión móvil**, active **Encriptación**.
3. Haga clic en **Seleccionar certificado** para abrir una lista de nombres de sujeto únicos de certificados que tienen una clave privada y que están instalados en el ordenador local en el almacenamiento de certificados de Windows.
4. Seleccione un certificado para encriptar la comunicación del cliente de XProtect Mobile y XProtect Web Client con el servidor móvil.

   Seleccione **Detalles** para ver la información del almacenamiento de certificados de Windows sobre el certificado seleccionado.

   El usuario del servicio Mobile Server ha recibido acceso a la clave privada. Es necesario que este

certificado sea de confianza en todos los clientes.



5. Haga clic en **Aplicar**.

Al aplicar certificados, el servidor de Mobile Server ere reinicia.

Milestone Federated Architecture

Configurar su sistema para ejecutar sitios federados

Para preparar su sistema para Milestone Federated Architecture, debe realizar ciertas elecciones cuando instale el servidor de gestión. Dependiendo de cómo esté configurada su infraestructura informática, elija entre tres alternativas diferentes.

Alternativa 1: Conectar sitios del 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 implicados en la jerarquía del sitio federado. La forma de conectar los sitios depende de la cuenta de usuario creada.

Con una cuenta de usuario de Windows

1. Inicie la instalación del producto en el servidor que se utilizará como servidor de gestión y seleccione **Personalizado**.
2. Seleccione para instalar el servicio Management Server utilizando una cuenta de usuario. La cuenta de usuario seleccionada debe ser la cuenta de administrador utilizada en todos los servidores de gestión. Debe utilizar la misma cuenta de usuario cuando instale los demás servidores de gestión en la jerarquía de sitios federados.
3. Finalizar la instalación. Repita los pasos 1 a 3 para instalar cualquier otro sistema que desee añadir a la jerarquía del sitio federado.
4. Añadir el sitio a la jerarquía (consulte Añadir sitio a la jerarquía en la página 320).

Con una cuenta de usuario integrada en Windows (servicio de red)

1. Inicie la instalación del producto en el primer servidor que se utilizará como servidor de gestión y seleccione **Ordenador único** o **Personalizado**. Esto instala el servidor de gestión utilizando una cuenta de servicio de red. Repita este paso para todos los sitios de su jerarquía de sitios federados.
2. Inicie sesión en el sitio que desee como sitio central en la jerarquía de sitios federados.
3. En el Management Client, expanda **Seguridad** > **Cometidos** > **Administradores**.
4. En la pestaña **Usuarios y grupos**, haga clic en **Añadir** y seleccione **Usuario de Windows**.
5. En el cuadro de diálogo, seleccione **Ordenadores** como tipo de objeto, introduzca el nombre del servidor del sitio federado y haga clic en **Aceptar** para añadir el servidor al cometido de **Administrador** del sitio central. Repita este paso hasta que haya añadido todos los sitios federados de esta manera y salga de la aplicación.
6. Inicie sesión en cada sitio federado y añada los siguientes servidores al cometido de **Administrador**, de la misma manera que en el caso anterior:
   - El servidor del sitio principal.
   - Los servidores del sitio secundario que desea conectar directamente a este sitio federado.
7. Añadir el sitio a la jerarquía (consulte Añadir sitio a la jerarquía en la página 320).

Alternativa 2: Conectar sitios de diferentes dominios

Para conectarse a sitios a través de dominios, asegúrese de que los dominios confían entre sí. Los dominios se configuran para que confíen unos en otros en la configuración del dominio de Microsoft Windows. Cuando se haya establecido la confianza entre los diferentes dominios en cada sitio en la jerarquía de sitios federados, siga la misma descripción como se describe en la alternativa 1. Para obtener más información sobre cómo configurar los dominios de confianza, consulte el sitio web de Microsoft (https://docs.microsoft.com/previous-versions/windows/it-pro/windows-2000-server/cc961481(v=technet.10)/).

Milestone recomienda Milestone Interconnect para crear sistemas multisitio conectados con múltiples dominios.

Alternativa 3: Conectar sitios en grupos de trabajo

Cuando conecte 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. Inicie sesión en **Windows** utilizando una cuenta de administrador común.
2. Inicie la instalación del producto y haga clic en **Personalizado**.
3. Seleccione para instalar el servicio Management Server utilizando la cuenta común de administrador.
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 común de administrador.
5. Añadir el sitio a la jerarquía (consulte Añadir sitio a la jerarquía en la página 320).

Milestone recomienda Milestone Interconnect para crear sistemas multisitio conectados cuando los sitios no forman parte de un dominio.

No puede mezclar dominio(s) y grupo(s) de trabajo. Esto significa que no puede conectar sitios de un dominio con sitios de un grupo de trabajo y viceversa.

Añadir sitio a la jerarquía

A medida que amplíe su sistema, puede añadir sitios a su sitio principal y a sus sitios secundarios, siempre que el sistema esté configurado correctamente.

Al agregar un sitio no seguro a Milestone Federated Architecture, asegúrese de que **Permitir conexiones no seguras al servidor** esté habilitado en **Herramientas** > **Opciones** > **Ajustes generales** en Management Client.

1. Seleccione el panel **Jerarquía de sitios federados**.
2. Seleccione el sitio al que desea añadir un sitio secundario, haga clic con el botón derecho y haga clic en **Añadir sitio a la jerarquía**.
3. Introduzca la URL del sitio solicitado en la ventana **Añadir sitio a la jerarquía** y haga clic en **Aceptar**.
4. El sitio principal envía una solicitud de enlace al sitio secundario y, al cabo de un tiempo, se añade un enlace entre los dos sitios al panel de **Jerarquía de sitios federados**.

5. Si puede establecer el enlace con el sitio secundario sin solicitar la aceptación del administrador del sitio secundario, vaya al paso 7.

   Si **no** es así, el sitio secundario tiene el icono de espera de aceptación hasta que el administrador del sitio secundario haya autorizado la solicitud.

6. Asegúrese de que el administrador del sitio secundario autoriza la solicitud de enlace desde el sitio principal (consulte Aceptar la inclusión en la jerarquía en la página 321).

7. El nuevo enlace principal/secundario se establece y el panel de **Jerarquía de sitios federados** se actualiza con el icono del nuevo sitio secundario.

Aceptar la inclusión en la jerarquía

Cuando un sitio secundario ha recibido una solicitud de enlace de un posible sitio principal en el que el administrador no tenía permisos de administrador para el sitio secundario, tiene el icono de esperando aceptación .

Para aceptar una solicitud de enlace:

1. Inicie sesión en el sitio.

2. En el panel de **Jerarquía de sitios federados**, haga clic con el botón derecho del ratón 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 derecho en el panel **Navegación del sitio**.

3. Haga clic en **Sí**.

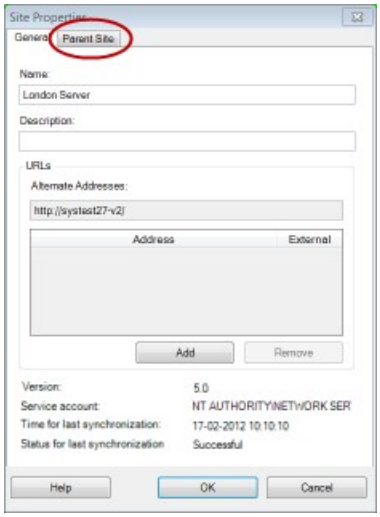
4. El nuevo enlace principal/secundario se establece y el panel de **Jerarquía de sitios federados** se actualiza con el icono del sitio normal para el sitio seleccionado.

> Los cambios que realice en los sitios hijos situados lejos del sitio principal pueden tardar en reflejarse en el panel de **Jerarquía de sitios federados**.

Establecer propiedades del sitio

Puede ver y, posiblemente, editar las propiedades de su sitio principal y sus sitios secundarios.

1. En el Management Client, en el panel de **Jerarquía de sitios federados**, seleccione el sitio correspondiente, haga clic con el botón derecho y seleccione **Propiedades**.



2. Si es necesario, cambie lo siguiente:

   Pestaña **General** (consulte Pestaña general en la página 621)

   Pestaña del **Sitio principal** (consulte Pestaña del sitio principal en la página 622) **(disponible solo en sitios secundarios)**

   > Debido a problemas de sincronización, cualquier cambio realizado en los secundarios remotos puede tardar en reflejarse en el panel de **Navegación del sitio**.

Actualizar jerarquía del sitio

El sistema sincroniza automáticamente de manera regular la jerarquía a través de todos los niveles de su configuración principal/secundario. Puede actualizarla manualmente, si quiere ver los cambios reflejados al instante en la jerarquía, y no quiere esperar a la siguiente sincronización automática.

Es necesario haber iniciado sesión en un sitio para realizar una actualización manual. Solo se reflejan los cambios guardados por este sitio desde la última sincronización mediante una actualización. Esto significa que los cambios realizados más abajo en la jerarquía podrían no ser reflejados por la actualización manual, si los cambios no han llegado aún al sitio.

1. Inicie sesión en el sitio correspondiente.
2. Haga clic con el botón derecho en el sitio superior del panel de **Jerarquía de sitios federados** y haga clic en **Actualizar jerarquía de sitios**.

   Esto tardará unos segundos.

Iniciar sesión en otros sitios de la jerarquía

Puede iniciar sesión en otros sitios y administrarlos. El sitio en el que ha iniciado sesión es su sitio inicial.

1. En el panel **Jerarquía de sitios federados**, haga clic con el botón derecho del ratón en el sitio en el que desea iniciar sesión.
2. Haga clic en **Iniciar sesión en el sitio**.

   El Management Client para ese sitio se abre.
3. Introduzca los datos de acceso y haga clic en **Aceptar**.
4. Una vez completado el inicio de sesión, podrá realizar sus tareas administrativas para ese sitio.

Actualizar la información de sitios secundarios

> Esta sección solo es relevante si utiliza XProtect Corporate o XProtect Expert 2014 o más reciente.

En una configuración grande de Milestone Federated Architecture con muchos sitios secundarios, es fácil perder la visión de conjunto y puede ser difícil encontrar la información de contacto de los administradores de cada sitio secundario.

Por lo tanto, puede añadir información adicional a cada sitio secundario y esta información estará disponible para los administradores en el sitio central.

Al detener el ratón sobre el nombre del sitio en el panel de **Jerarquía de sitios federados**, podrá leer la información sobre el sitio. Para actualizar la información sobre el sitio:

1. Inicie sesión en el sitio.
2. Haga clic en el panel **Navegación del sitio** y seleccione **Información del sitio**.
3. Haga clic en **Editar** y añada la información correspondiente en cada categoría.

Separar un sitio de la jerarquía

Cuando desvincula un sitio de su sitio principal, el vínculo entre los sitios se rompe. Puede desvincular sitios del sitio central, del propio sitio o de su sitio principal.

1. En el panel de **Jerarquía de sitios federados**, haga clic con el botón derecho en el sitio y haga clic en **Separar sitio de la jerarquía**.
2. Haga clic en **Sí** para actualizar el panel de **Jerarquía de sitios federados**.

   Si el sitio separado tiene sitios secundarios, se convierte en el nuevo sitio principal para esta rama de la jerarquía, y el icono del sitio normal cambia a un icono de sitio principal .
3. Haga clic en **Aceptar**.

Los cambios en la jerarquía se reflejan tras una actualización manual o una sincronización automática.

Milestone Interconnect

Añadir un sitio remoto a su sitio central Milestone Interconnect

Los sitios remotos se añaden al sitio central con el asistente **Añadir hardware**.
Requisitos

- Suficientes licencias de cámara de Milestone Interconnect (consulte Milestone Interconnect y licencia en la página 94).
- Otro sistema XProtect configurado y en funcionamiento que incluya una cuenta de usuario (usuarios básicos, usuario local de Windows o usuario del Active Directory de Windows) con permisos para los dispositivos a los que el sistema central de XProtect Corporate debe poder acceder
- Conexión de red entre el sitio central XProtect Corporate y los sitios remotos con acceso o reenvío de puertos a los puertos utilizados 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 **Generalidades**, expanda el servidor de grabación correspondiente y haga clic con el botón derecho.
3. Seleccione **Añadir hardware** para iniciar el asistente.
4. En la primera página seleccione **Escaneo de rango de direcciones** o **Manual** y haga clic en **Siguiente**.
5. Especifique los nombres de usuario y las contraseñas. La cuenta de usuario debe estar predefinida en el sistema remoto. Puede añadir los nombres de usuario y las contraseñas que necesite haciendo clic en **Añadir**. Cuando esté a punto, haga clic en **Siguiente**.
6. Seleccione los drivers a utilizar cuando escanee. En este caso, elija entre los drivers Milestone. Haga clic en **Siguiente**.
7. Especifique las direcciones IP y los números de puerto que desea escanear. El puerto por defecto es 80. Haga clic en **Siguiente**.

   Espere mientras su sistema detecta los sitios remotos. Un indicador de estado muestra el proceso de detección. En caso de que una detección sea exitosa, aparece un mensaje de **Éxito** en la columna de **Estado**. Si no se puede añadir, puede hacer clic en el mensaje de error **Fallido** para ver el motivo.
8. Elija habilitar o deshabilitar 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. Elija habilitar o deshabilitar el hardware y los dispositivos detectados correctamente. Haga clic en **Siguiente**.

11. Seleccione un grupo por defecto. Haga clic en **Finalizar**.
12. Después de la instalación, puede ver el sistema y sus dispositivos en el panel de **Generalidades**.

    Dependiendo de los permisos del usuario seleccionado en el sitio remoto, el sitio central obtiene acceso a todas las cámaras y funciones o a un subconjunto de ellas.

Asignar permisos de usuario

Configura los permisos de usuario para una cámara interconectada como lo hace con otras cámaras, creando un cometido y asignando acceso a las funciones.

1. En el sitio central, en el panel **Navegación del sitio**, expanda **Seguridad** y seleccione **Cometidos**.
2. En el panel Generalidades, haga clic con el botón derecho del ratón en el cometido de administrador incorporado y seleccione **Añadir cometido** (consulte y gestionar un cometido).
3. Dé un nombre al cometido y configure los ajustes en la pestaña **Dispositivo** (consulte la pestaña Dispositivo (roles)) y en la pestaña **Grabaciones remotas** (consulte la pestaña Grabaciones remotas (roles)).

Actualizar el hardware del sitio remoto

Si la configuración se ha modificado en un sitio remoto, por ejemplo, se han añadido o eliminado cámaras y eventos, debe 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 **Generalidades** expanda el servidor de grabación requerido, seleccione el sistema remoto correspondiente. Haz clic con el botón derecho.
3. Seleccione **Actualizar hardware**. Se abre el cuadro de diálogo **Actualizar hardware**.
4. El cuadro de diálogo enumera todos los cambios (dispositivos eliminados, actualizados y añadidos) en el sistema remoto desde la última vez que se estableció o actualizó la configuración Milestone Interconnect. Haga clic en **Confirmar** para actualizar su sitio central con estos cambios.

Habilitar la reproducción directamente desde la cámara del sitio remoto

Si su sede central está continuamente conectada con sus sedes remotas, puede configurar su sistema para que los usuarios reproduzcan las grabaciones directamente desde las sedes remotas. Si desea más información, consulte Milestone Interconnect ajustes (explicación) en la página 94.

1. En el sitio central, expanda **Servidores** y seleccione **Servidores de grabación**.
2. En el panel **Generalidades** expanda el servidor de grabación requerido, seleccione el sistema remoto correspondiente. Seleccione la cámara interconectada correspondiente.
3. En el panel Propiedades, seleccione la pestaña **Grabar**, y seleccione la opción **Reproducir 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, deberá redefinirlas en el sitio central.

Recuperar grabaciones a distancia de la cámara del sitio remoto

Si su sitio central **no** está conectado continuamente con sus sitios remotos, puede configurar su sistema para almacenar las grabaciones remotas de forma centralizada y puede configurar la recuperación de las grabaciones remotas cuando la conexión de red sea óptima. Si desea más información, consulte Milestone Interconnect ajustes (explicación) en la página 94.

Para permitir a los usuarios recuperar realmente las grabaciones, debe habilitar este permiso para el cometido correspondiente (consulte Cometidos (Seguridad)).

Para configurar su sistema:

1. En el sitio central, expanda **Servidores** y seleccione **Servidores de grabación**.
2. En el panel **Generalidades** expanda el servidor de grabación requerido, seleccione el sistema remoto correspondiente. Seleccione el servidor remoto correspondiente.
3. En el panel Propiedades, seleccione la pestaña **Recuperación remota** y actualice los ajustes (consulte Pestaña Recuperación remota en la página 448).

Si la red falla por alguna razón, el sitio central pierde las secuencias de grabación. Puede configurar su sistema para que el sitio central recupere automáticamente las grabaciones remotas para cubrir el período de inactividad, una vez que se restablezca la red.

1. En el sitio central, expanda **Servidores** y seleccione **Servidores de grabación**.
2. En el panel **Generalidades** expanda el servidor de grabación requerido, seleccione el sistema remoto correspondiente. Seleccione la cámara correspondiente.
3. En el panel Propiedades, seleccione la pestaña **Grabar** y seleccione la opción **Recuperar automáticamente las grabaciones remotas cuando se restablezca la conexión** (consulte Guardar y recuperar la grabación remota).
4. En la barra de herramientas, haga clic en **Guardar**.

Como alternativa, puede utilizar reglas o iniciar recuperaciones de grabaciones remotas desde 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, deberá redefinirlas en el sitio central.

Configurar el sitio central para que responda a los eventos de los sitios remotos

Puede utilizar eventos definidos en los sitios remotos para activar reglas y alarmas en su sitio central y así responder inmediatamente a los eventos de los sitios remotos. Esto requiere que los sitios remotos estén conectados y en línea. El número y el tipo de eventos dependen de los eventos configurados y predefinidos en los sitios remotos.

La lista de eventos subvencionados está disponible en el sitio web Milestone (https://www.milestonesys.com/).

No puede eliminar los eventos predefinidos.

Requisitos:

- Si desea utilizar eventos definidos por el usuario/manuales de los sitios remotos como eventos activadores, debe crearlos primero en los sitios remotos
- Asegúrese de tener una lista actualizada de los eventos de los sitios remotos (consulte Actualizar el hardware del sitio remoto en la página 325).

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 Generalidades, seleccione el servidor remoto correspondiente y la **pestaña Eventos**.
3. La lista contiene los eventos predefinidos. Haga clic en **Añadir** para incluir en la lista eventos definidos por el usuario o manuales del sitio remoto.

Utilice un evento en un sitio remoto para activar una alarma en el sitio central:

1. En el sitio central, expanda **Alarmas** y seleccione **Definiciones de alarmas**.
2. En el panel Generalidades, haga clic con el botón derecho **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 los definidos por el usuario que se admiten.
5. En el campo **Fuentes**, seleccione el servidor remoto que representa el sitio remoto desde el que desea recibir alarmas.
6. Guarde la configuración cuando haya terminado.

Utilice un evento en un sitio remoto para activar una acción basada en reglas en el sitio central:

1. En el sitio central, expanda **Reglas y eventos** y seleccione **Reglas**.
2. En el panel Generalidades, haga clic con el botón derecho **Reglas** y haga clic en **Añadir regla**.
3. En el asistente que aparece, seleccione **Realizar una acción en <evento>**.
4. En el área **Editar la descripción de la regla**, haga clic en **evento** y seleccione entre los eventos predefinidos y los definidos por el usuario. Haga clic en **Aceptar**.
5. Haga clic en **dispositivos/servidor de grabación/servidor de gestión** y seleccione el servidor remoto que representa el sitio remoto para el que desea que el sitio central inicie una acción. Haga clic en **Aceptar**.
6. Haga clic en **Siguiente** para pasar 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 el área **Editar descripción de la regla**. Haga clic en **Siguiente**.
9. Seleccione un criterio de detención si es necesario. Haga clic en **Siguiente**.
10. Seleccione una acción de detención si es necesario. Haga clic en **Finalizar**.

Servicios de conexión remota

Servicios de conexión remota (explicación)

> La funcionalidad disponible depende del sistema que esté utilizando. Vea la lista completa de características, que está disponible en la página de descripción del producto en el sitio web Milestone (https://www.milestonesys.com/solutions/platform/product-index/).

La característica de servicios de conexión remota contiene la tecnología de conexión de cámaras Axis One-click desarrollada por Axis Communications. Habilita al sistema a recuperar el vídeo (y el audio) de las cámaras externas cuando los cortafuegos y/o la configuración de la red del router impiden normalmente iniciar las conexiones con dichas cámaras. La comunicación real tiene lugar a través de servidores de túnel seguros (servidores ST). Los servidores ST utilizan VPN. Solo los dispositivos que poseen una clave válida funcionan dentro de una VPN. Esto ofrece un túnel seguro donde las redes públicas pueden intercambiar datos de forma segura.

Servicios de conexión remota (explicación)

- Editar las credenciales dentro del Servicio de despacho Axis
- Añadir, editar y eliminar servidores ST
- Registro/desregistro y edición de cámaras Axis One-click

- Vaya al hardware relacionado con la cámara Axis One-Click

Instalar un entorno de servidor de túnel seguro para la conexión de la cámara con un solo clic

Antes de poder utilizar la conexión de cámara Axis One-click, debe instalar un entorno de servidor ST adecuado. Para trabajar con entornos de servidor de túnel seguro (servidor ST) y cámaras Axis One-click, primero debe ponerse en contacto con su proveedor de sistemas para obtener el nombre de usuario y la contraseña necesarios para Axis Dispatch Services.

Requisitos

- Póngase en contacto con su proveedor de sistemas para obtener el nombre de usuario y la contraseña necesarios para Axis Dispatch Services
- Asegúrese de que su(s) cámara(s) es(son) compatible(s) con el sistema de hosting de vídeo de Axis. Vaya al sitio web de Axis para ver los dispositivos compatibles (https://www.axis.com/products/axis-guardian)
- Si es necesario, actualice sus cámaras Axis con el firmware más reciente. Vaya al sitio web de Axis para descargar el firmware (https://www.axis.com/support/firmware)

1. En la página de inicio de cada cámara, vaya a **Configuración básica**, **TCP/IP**, y seleccione **Habilitar AVHS** y **Siempre**.
2. Desde su servidor de gestión, vaya a la página de descargas de Milestone (https://www.milestonesys.com/downloads/) y descargue el software **AXIS One-Click**. Ejecute el programa para configurar un marco de túnel seguro de Axis adecuado.

Añadir o editar servidores de túneles seguros

La comunicación para los servicios de conexión remota tiene lugar a través de servidores seguros de túnel (servidores ST).

1. Haga una de las siguientes cosas:
   - Para añadir un servidor ST, haga clic con el botón derecho del ratón en el nodo superior **Servidores de túnel seguro Axis**, seleccione **Añadir servidor de túnel seguro Axis**
   - Para editar un servidor ST, haga clic con el botón derecho del ratón, seleccione **Editar servidor de túnel seguro Axis**
2. En la ventana que se abre, rellene la información correspondiente.
3. Si eligió utilizar credenciales cuando instaló el **componente Axis One-Click Connection**, seleccione la casilla de verificación **Utilizar credenciales** e introduzca el mismo nombre de usuario y contraseña que utilizó para el **componente Axis One-Click Connection**.
4. Haga clic en **Aceptar**.

Registrar una nueva cámara Axis One-Click

1. Para registrar una cámara en un servidor ST, haga clic con el botón derecho del ratón y seleccione **Registrar cámara Axis One-Click**.
2. En la ventana que se abre, rellene la información correspondiente.
3. Haga clic en **Aceptar**.
4. La cámara aparece ahora bajo el servidor ST correspondiente.

La cámara puede tener la siguiente codificación de colores:

Color	Descripción
Rojo	Estado inicial. Registrado, pero no conectado al servidor ST.
Amarillo	Registrado. Conectado al servidor ST, pero no añadido como hardware.
Verde	Añadido como hardware. Puede o no estar conectado al servidor ST.

Cuando se añade una nueva cámara, su estado es siempre verde. El estado de la conexión se refleja en **Dispositivos** en los **Servidores de grabación** en el panel **Generalidades**. En el panel **Generalidades**, puede agrupar sus cámaras para obtener una visión general más sencilla. Si elige **no** registrar su cámara en el servicio de envío de Axis en este momento, puede hacerlo más tarde desde el menú del botón derecho (seleccione **Editar cámara Axis One-Click**).

Planos inteligente

Entornos geográficos (explicación)

Antes de que un usuario de XProtect Smart Client pueda seleccionar un fondo geográfico, primero debe configurar los fondos geográficos en XProtect Management Client.

- **Mapamundi básico** - Usa el entorno geográfico estándar proporcionado en XProtect Smart Client. No requiere ninguna configuración. 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

- **Milestone Map Service** - conecta a un proveedor de planos gratuito. Después de habilitarlo Milestone Map Service, no es necesaria ninguna otra configuración.

  Consulte Habilitar Milestone Map Service

- **OpenStreetMap** conecta a:
  - Un servidor de archivos comerciales de su elección
  - Su propio servidor local de archivos

  Consulte Especifique el servidor de fichas OpenStreetMap

Las opciones de Bing Maps y Google Maps requieren acceso a Internet, y debe adquirir una clave de Microsoft o Google.

Milestone Map Service requiere acceso a Internet.

A menos que utilice su propio servidor de fichas local, OpenStreetMap requiere acceso a Internet.

Si desea que el sistema tenga una instalación que cumpla con el RGPD de la UE, no podrá utilizar los siguientes servicios:

- Bing Maps
- Google Maps
- Milestone Map Service

Para obtener más información sobre la protección de datos y la recopilación de datos de uso, consulte la guía de privacidad del RGPD.

De manera predeterminada, Bing Maps y Google Maps muestran imágenes del satélite. Puede cambiar las imágenes en XProtect Smart Client, por ejemplo a aéreas o terrestres, para ver diferentes detalles.

Habilitar Bing Maps o Google Maps en Management Client

Puede hacer que una clave esté disponible para varios usuarios introduciéndola para un perfil Smart Client en Management Client. Todos los usuarios asignados al perfil utilizarán esta clave.

Pasos:

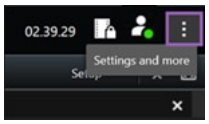
1. En Management Client, en el panel de **Navegación del sitio**, haga clic en **Perfiles Smart Client**.
2. En el panel **Perfiles Smart Client**, selecione el perfil Smart Client deseado.
3. En el panel **Propiedades**, haga clic en la pestaña **Plano inteligente**:
   - Para Bing Maps, introduzca su Clave básica o Clave empresarial en el campo de la **clave de Bing Maps**
   - Para Google Maps, introduzca su clave Maps Static API en el campo **Clave privada para Google Maps**
4. Para evitar que los operadores de XProtect Smart Client utilicen una tecla diferente, seleccione la casilla **Bloqueado**.

Habilitar Bing Maps o Google Maps en XProtect Smart Client

Para que los operadores XProtect Smart Client puedan utilizar una clave diferente a la del perfil Smart Client, debe introducir la clave en los ajustes de XProtect Smart Client.

Pasos:

1. En XProtect Smart Client, abra la ventana **Ajustes**.



2. Haga clic en **Plano inteligente**.
3. Dependiendo del servicio de planos que quieras utilizar, haz una de las siguientes cosas:
   - Para Bing Maps, introduzca su clave en el **Bing Maps campo** clave. Consulte también Integración de planos inteligentes con Bing Maps (explicación) en la página 90.
   - Para Google Maps, introduzca su clave en el campo **Clave privada para Google Maps**. Consulte también Integración de planos inteligentes con Google Maps (explicación) en la página 89.

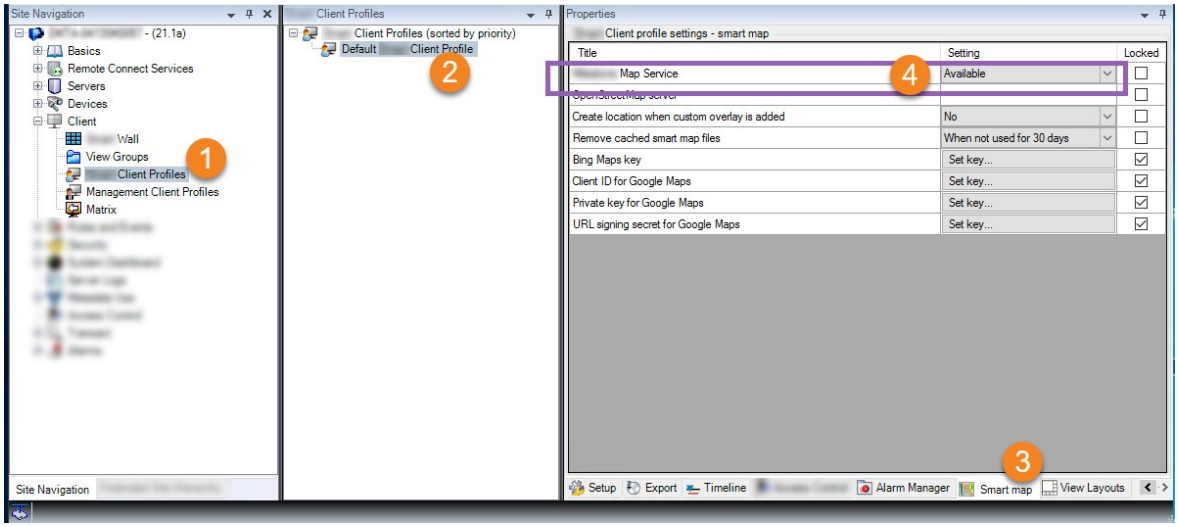
Habilitar Milestone Map Service

Milestone Map Service es un servicio en línea que le permite conectarse al servidor de azulejos de Milestone Systems. Este servidor de archivos utiliza un servicio de planos gratuito y disponible en el mercado.

Una vez habilitado Milestone Map Service en su plano inteligente, el plano inteligente utilizará Milestone Map Service como fondo geográfico.

Pasos:

1. En el panel de **Navegación del sitio**, expanda el nodo **Cliente** haga clic en **Perfiles Smart Client**.
2. En el panel de generalidades, seleccione el perfil Smart Client correspondiente.
3. En el panel **Propiedades**, haga clic en la pestaña **Plano inteligente**.



4. En el campo **Milestone Map Service**, seleccione **Disponible**.
5. Para aplicar esta configuración en XProtect Smart Client, seleccione la casilla **Bloqueado**. Entonces los operadores XProtect Smart Client no pueden habilitar o deshabilitar Milestone Map Service.
6. Guardar los cambios.

También puede habilitar Milestone Map Service en la ventana de **Ajustes** en XProtect Smart Client.

Milestone Map Service requiere acceso a Internet.

Si está detrás de un cortafuegos restrictivo, es importante permitir el acceso a los dominios utilizados. Es posible que tenga que permitir el tráfico saliente para Milestone Map Service utilizando maps.milestonesys.com en cada máquina en la que se ejecute el Smart Client.

Especificar servidor de fichas OpenStreetMap

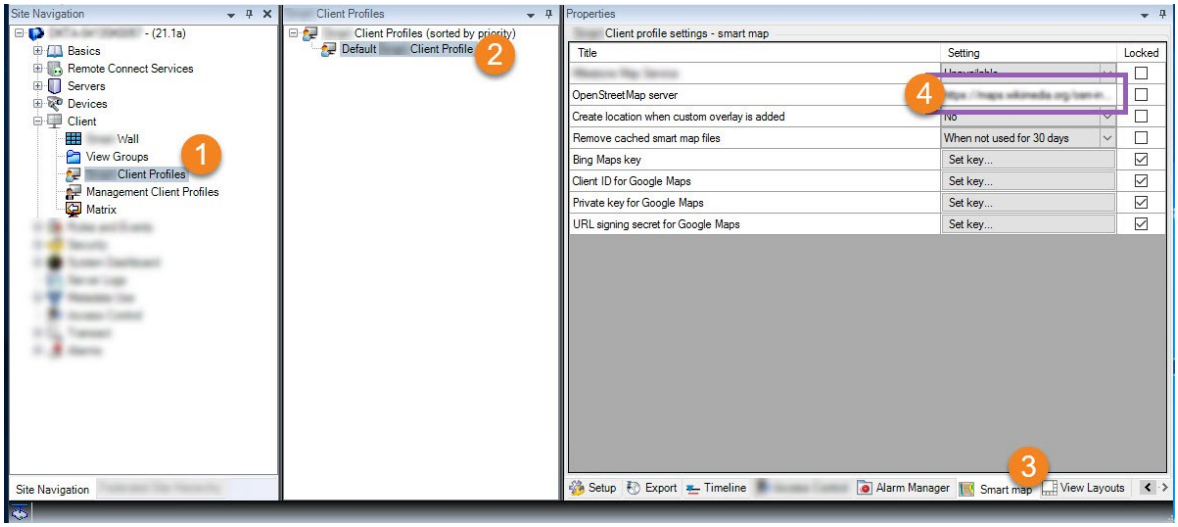
Si utiliza la opción **OpenStreetMap** como fondo geográfico para su plano inteligente, deberá especificar de dónde se recuperan las imágenes en mosaico. Para ello, hay que especificar la dirección del servidor de fichas, ya sea un servidor de fichas comercial o un servidor de fichas local, por ejemplo, si su organización tiene sus

propios planos para zonas como aeropuertos o puertos.

> También puede especificar la dirección del servidor de fichas en la ventana de **Ajustes** en XProtect Smart Client.

Pasos:

1. En el panel de **Navegación del sitio**, expanda el nodo **Cliente** haga clic en **Perfiles Smart Client**.
2. En el panel de generalidades, seleccione el perfil Smart Client correspondiente.
3. En el panel **Propiedades**, haga clic en la pestaña **Plano inteligente**.



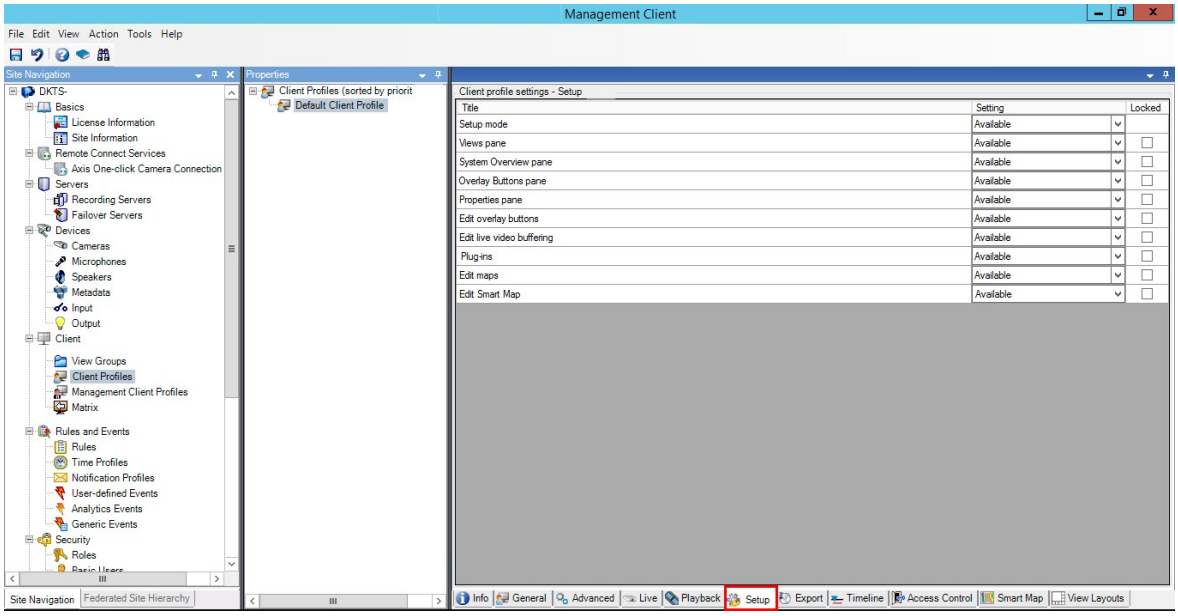
4. En el campo del **servidor de OpenStreetMap**, introduzca la dirección del servidor de fichas.
5. Para aplicar esta configuración en XProtect Smart Client, seleccione la casilla **Bloqueado**. Entonces los operadores de XProtect Smart Client no pueden cambiar la dirección.
6. Guardar los cambios.

Habilitar la edición de planos inteligentes

Los operadores pueden editar los planos inteligentes en XProtect Smart Client en el modo de configuración solo si la edición está habilitada en Management Client. Si no está habilitado, debe habilitar la edición para cada perfil de Smart Client relevante.

Pasos:

1. En el panel de **Navegación del sitio**, expanda el nodo **Cliente**.
2. Haga clic en **Perfiles Smart Client**.



3. En el panel de generalidades, seleccione el perfil Smart Client correspondiente.
4. En el panel **Propiedades**, haga clic en la pestaña **Configuración**.
5. En la lista **Editar plano inteligente**, seleccione **Disponible**.
6. Repita estos pasos para cada perfil de Smart Client correspondiente.
7. Guarde sus cambios. La próxima vez que los usuarios asignados al perfil Smart Client seleccionado inicien sesión en XProtect Smart Client, podrán editar los planos inteligentes.

Para desactivar la edición, en la lista **Editar plano inteligente**, seleccione **No disponible**.

Habilitar la edición de dispositivos en el plano inteligente

Debe habilitar la edición de dispositivos por rol para permitir a los operadores, por ejemplo:

- Posicione un dispositivo de entrada o un micrófono en un plano inteligente
- Ajustar el campo de visión de una cámara en un plano inteligente

Los operadores pueden editar los siguientes tipos de dispositivos en los planos inteligentes:

- Cámaras
- Dispositivos de entrada
- Micrófonos

Requisitos
Antes de empezar, asegúrese de que se ha habilitado la edición de planos inteligentes (consulte Habilitar la edición de planos inteligentes en la página 334). Esto se hace en el perfil Smart Client al que está asociado el cometido del operador.

Pasos:

1. Expanda el nodo de **Seguridad** > **Cometidos**.
2. En el panel **Cometidos**, seleccione el cometido al que está asociado su operador.
3. Para dar al cometido permisos de edición:
    - Seleccione la pestaña **Seguridad general** y, en el panel **Ajustes de cometido**, seleccione el tipo de dispositivo (por ejemplo, **Cámaras** o **Entrada**)
    - En la columna **Permitir**, seleccione la casilla **Control total** o **Editar**
4. Guardar los cambios.

Para habilitar la edición de dispositivos individuales, vaya a la pestaña **Dispositivo** y seleccione el dispositivo correspondiente.

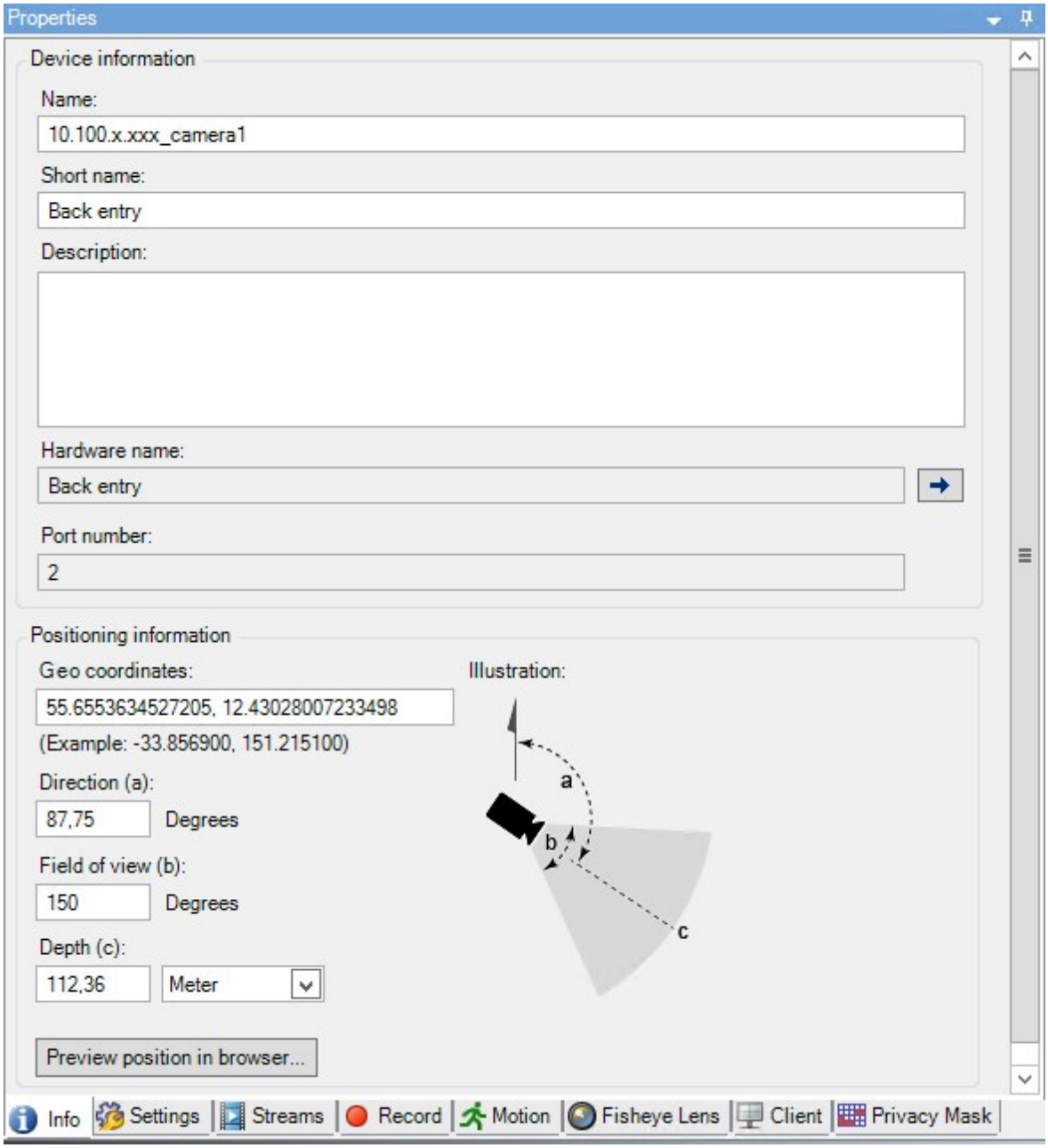
Defina la posición del dispositivo y la dirección de la cámara, el campo de visión y la profundidad (plano inteligente)

Para garantizar que un dispositivo está correctamente posicionado en el plano inteligente, puede establecer las coordenadas geográficas del mismo. En el caso de las cámaras, también se puede ajustar la dirección, el campo de visión y la profundidad de visualización. La configuración de cualquiera de las opciones anteriores añadirá automáticamente el dispositivo al plano inteligente la próxima vez que un operador cargue el plano inteligente en XProtect Smart Client.

Pasos:

1. En Management Client, expanda el nodo **Dispositivos** y seleccione el tipo de dispositivo (por ejemplo, **Cámaras** o **Entrada**).
2. En el panel **Dispositivos**, seleccione el dispositivo correspondiente.

3. En la pestaña **Información**, desplácese abajo hasta **Información de posicionamiento**.



4. En el campo **Coordenadas geográficas**, especifique las coordenadas de latitud y longitud, en ese orden. Utilice un punto como separador de decimales, y use una coma para separar la latitud y la longitud.

- Para cámaras:
    1. En el campo **Dirección**, introduzca un valor en el rango de 0 y 360 grados.
    2. En el campo **Campo de visión**, introduzca un valor en el rango de 0 y 360 grados.
    3. En el campo **Profundidad**, introduzca la profundidad de visualización, en metros o en pies.

5. Guardar los cambios.

También puede establecer las propiedades en los servidores de grabación.

Configurar el plano inteligente con Milestone Federated Architecture

Cuando utiliza un plano inteligente en un Milestone Federated Architecture, todos los dispositivos de los sitios conectados aparecen en el plano inteligente. Siga los siguientes pasos para configurar el plano inteligente en una arquitectura federada.

Para obtener información general sobre Milestone Federated Architecture, consulte Configuración de Milestone Federated Architecture en la página 95.

1. Antes de conectar el sitio superior con los sitios secundarios, asegúrese de que se han especificado las coordenadas geográficas en todos los dispositivos de todos los sitios. Las coordenadas geográficas se añaden automáticamente cuando un dispositivo se posiciona en el plano inteligente en XProtect Smart Client, pero también puede añadirlas manualmente en Management Client en las propiedades del dispositivo. Si desea más información, consulte Defina la posición del dispositivo y la dirección de la cámara, el campo de visión y la profundidad (plano inteligente) en la página 336.
2. Debe añadir a los operadores Smart Client como usuarios de Windows en el sitio principal y en todos los sitios federados. Al menos en el sitio superior, los usuarios de Windows deben tener permisos de edición de planos inteligentes. Esto permite a los usuarios editar el plano inteligente para el sitio superior y para todos los sitios secundarios. A continuación, debe determinar si los usuarios de Windows de los sitios secundarios necesitan permisos de edición de planos inteligentes. En Management Client, primero crea los usuarios de Windows en **Cometidos**, y luego se habilita la edición de planos inteligentes. Si desea más información, consulte Habilitar la edición de planos inteligentes en la página 334.
3. En el sitio superior, añada los sitios secundarios como usuarios de Windows a un cometido con permisos de administrador. Cuando especifique el tipo de objeto, seleccione la casilla **Ordenadores**.
4. En cada sitio secundario, añada el sitio superior como usuario de Windows con el mismo cometido de administrador que se utiliza en el sitio superior. Cuando especifique el tipo de objeto, seleccione la casilla **Ordenadores**.

5. En el sitio superior, asegúrese de que puede ver la ventana de **Jerarquía de sitios federados**. En Management Client, vaya a **Vista** y seleccione **Jerarquía de sitios federados**. Añade cada uno de los sitios secundarios al sitio superior. Si desea más información, consulte Añadir sitio a la jerarquía en la página 320.
6. Ahora puede probar Milestone Federated Architecture funciona en XProtect Smart Client. Inicie sesión en el sitio superior como administrador o como operador, y abra una vista que contenga el plano inteligente. Si la configuración se ha realizado correctamente, todos los dispositivos del sitio superior y de los sitios secundarios aparecen en el plano inteligente. Si inicia sesión en uno de los sitios secundarios, solo verá los dispositivos de ese sitio y sus sitios secundarios.

Para editar dispositivos en un plano inteligente, por ejemplo la posición y el ángulo de la cámara, los usuarios necesitan permisos de edición de dispositivos. Si desea más información, consulte Habilitar la edición de dispositivos en el plano inteligente en la página 335.

Mantenimiento

Hacer una copia de seguridad y restaurar la configuración del sistema

Milestone recomienda hacer copias de seguridad periódicas de la configuración del sistema como medida de recuperación ante desastres.

Aunque es raro perder la configuración, puede ocurrir en circunstancias desafortunadas. Es importante que proteja sus copias de seguridad, ya sea con medidas técnicas u organizativas.

Hacer una copia de seguridad y restaurar la configuración del sistema (explicación)

El sistema ofrece una función integrada que hace una copia de seguridad de toda la configuración del sistema que se puede definir en el Management Client. La base de datos del servidor de registro y los archivos de registro, incluidos los archivos de registro de auditoría, no se incluyen en esta copia de seguridad.

Si su 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.

Hacer una copia de seguridad de la configuración del sistema puede llevar algún tiempo. La duración de la copia de seguridad depende de:

- La configuración de su sistema
- Su hardware
- Si ha instalado el componente SQL Server, componente Event Server y el componente de Management Server en un solo servidor o en varios

Cada vez que se realiza una copia de seguridad, tanto manual como programada, se vacía el archivo de registro de transacciones de la base de datos SQL. Para obtener información adicional sobre cómo vaciar el archivo de registro de transacciones, consulte Registro de transacciones de la base de datos SQL (explicación) en la página 138.

> ⚠ Asegúrese de conocer los ajustes de la contraseña de configuración del sistema cuando cree una copia de seguridad.

En el caso de los sistemas que cumplan con FIPS 140-2, con exportaciones y bases de datos de medios archivados de versiones de XProtect VMS anteriores a 2017 R1 que estén cifrados con cifrados que no cumplan con FIPS, es necesario archivar los datos en una ubicación en la que se pueda seguir accediendo a ellos después de habilitar FIPS. Para obtener información detallada sobre cómo configurar su XProtect VMS para que se ejecute en modo compatible con FIPS 140-2, consulte la sección de cumplimiento de FIPS 140-2 la guía de endurecimiento.

Seleccionar la carpeta de copia de seguridad compartida

Antes de realizar una copia de seguridad y restaurar cualquier configuración del sistema, debe establecer una carpeta de copia de seguridad para este fin.

1. Haga clic con el botón derecho en el icono de servicio del área de notificación de Management Server y seleccione **Seleccione la carpeta de copia de seguridad compartida**.
2. En la ventana que aparece, busque la ubicación del archivo deseado.
3. Haga clic en **Aceptar** dos veces.
4. Si se le pregunta si desea eliminar los archivos de la carpeta de copia de seguridad actual, haga clic en **Sí** o en **No**, dependiendo de sus necesidades.

Hacer una copia de seguridad manual de la configuración del sistema

1. En la barra de menú, seleccione **Archivo** > **Configuración de copia de seguridad**.
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. Introduzca el destino de la carpeta y haga clic en **Guardar**.
5. Espere a que termine la copia de seguridad y haga clic en **Cerrar**.

Todos los archivos de configuración del sistema correspondientes se combinan en un único archivo .cnf que se guarda en una ubicación determinada. Durante la copia de seguridad, todos los archivos de copia de seguridad se exportan primero a una carpeta temporal de copia de seguridad del sistema en el servidor de gestión. Puede seleccionar otra carpeta temporal haciendo clic con el botón derecho en el icono de servicio del área de notificación Management Server y seleccionando Seleccionar carpeta de copia de seguridad compartida.

Restaurar la configuración del sistema a partir de una copia de seguridad manual

Información importante

- Tanto el usuario que instala como el que restaura deben ser administradores locales de la base de datos SQL de configuración del sistema en el servidor de gestión **y** en el SQL Server
- A excepción de sus servidores de grabación, su sistema estará completamente apagado mientras dure la restauración, que puede llevar algún tiempo
- Una copia de seguridad solo puede restaurarse en la instalación del sistema donde se creó. Asegúrese de que la configuración es lo más parecida posible a cuando se hizo la copia de seguridad. De lo contrario, la restauración podría fallar
- Si se le pide una contraseña de configuración del sistema durante una restauración, debe proporcionar la contraseña de configuración del sistema que era válida en el momento en que se creó la copia de seguridad. Sin esta contraseña, no podrá restaurar su configuración a partir de la copia de seguridad
- Si hace una copia de seguridad de la base de datos SQL y la restaura en una SQL Server limpia, entonces los errores de elevación de la base de datos SQL no funcionarán y solo recibirá un mensaje de error genérico del SQL Server. Para evitarlo, primero reinstale su sistema XProtect usando el SQL Server limpio y a continuación restaure la copia de seguridad sobre ella
- Si la restauración falla durante la fase de validación, puede volver a iniciar la configuración antigua porque no ha realizado ningún cambio
  Si la restauración falla en otra parte del proceso, no podrá volver a la configuración anterior
  Mientras el archivo de copia de seguridad no esté dañado, puede realizar otra restauración
- La restauración reemplaza la configuración actual. Esto significa que cualquier cambio en la configuración desde la última copia de seguridad se pierde
- No se restauran los registros, incluidos los de auditoría
- Una vez iniciada la restauración, no se puede cancelar

Restaurando

1. Haga clic con el botón derecho en el icono de servicio del área de notificación de Management Server y seleccione **Restaurar configuración**.
2. Lea la nota importante y haga clic en **Restaurar**.
3. En el cuadro de diálogo de apertura de archivos, busque la ubicación del archivo de copia de seguridad de la configuración del sistema, selecciónelo y haga clic en **Abrir**.

   El archivo de copia de seguridad está ubicado en el ordenador Management Client. Si el Management Client está instalado en un servidor diferente, copie el archivo de copia de seguridad a este servidor antes de seleccionar el destino.

4. Se abre la ventana **Restaurar configuración**. Espere a que acabe la restauración y haga clic en **Cerrar**.

Contraseña de configuración del sistema (explicación)

Puede optar por proteger la configuración general del sistema asignando una contraseña de configuración del sistema. Después de asignar una contraseña de configuración del sistema, las copias de seguridad están protegidas por esta contraseña. La configuración de la contraseña se almacena en el ordenador que ejecuta el servidor de gestión en una carpeta segura. Necesitará esta contraseña para:

- Restaurar la configuración a partir de una copia de seguridad de la configuración que se creó con ajustes de contraseña diferentes a los actuales
- Mover o instalar el servidor de gestión en otro ordenador debido a un fallo de hardware (recuperación)
- Configurar un servidor de gestión adicional en un sistema con clustering

La contraseña de configuración del sistema se puede asignar durante la instalación o después de la misma. La contraseña debe cumplir con los requisitos de complejidad de Windows, que están definidos por la política de Windows para las contraseñas.

Es importante que los administradores del sistema guarden esta contraseña y la mantengan a salvo. Si ha asignado una contraseña de configuración del sistema y está restaurando una copia de seguridad, es posible que se le pida la contraseña de configuración del sistema. Sin esta contraseña, no podrá restaurar su configuración a partir de la copia de seguridad.

Ajustes de la contraseña de configuración del sistema

Se pueden cambiar los ajustes de la contraseña de configuración del sistema. En la configuración de la contraseña del sistema, tiene estas opciones:

- Elija proteger con contraseña la configuración del sistema asignando una contraseña de configuración del sistema
- Cambiar una contraseña de configuración del sistema
- Elija no proteger con contraseña la configuración del sistema eliminando cualquier contraseña de configuración del sistema asignada

Cambiar los ajustes de contraseña de la configuración del sistema

Al cambiar la contraseña, es importante que los administradores del sistema guarden las contraseñas asociadas a las diferentes copias de seguridad y las mantengan a salvo. Si está restaurando una copia de seguridad, es posible que se le pida la contraseña de configuración del sistema que era válida en el momento en que se creó la copia de seguridad. Sin esta contraseña, no podrá restaurar su configuración a partir de la copia de seguridad.

Después de cambiar la contraseña, y si su servidor de gestión y su servidor de eventos están instalados en ordenadores distintos, deberá introducir también la contraseña de configuración actual del sistema en el servidor de eventos. Para obtener más información, consulte Introducir la contraseña de configuración actual del sistema (servidor de eventos).

Para aplicar los cambios, debe reiniciar los servicios del servidor de gestión.

1. Localice el icono de la bandeja del servidor de gestión y asegúrese de que el servicio se está ejecutando.
2. Haga clic con el botón derecho en el icono de servicio del área de notificación de Management Server y seleccione **Cambiar la configuración de la contraseña del sistema**.
3. Aparece la ventana de cambio de contraseña de ajustes de la configuración del sistema.

Asignar una contraseña

1. Escriba la nueva contraseña en el campo **Nueva contraseña**.
2. Vuelva a escribir la nueva contraseña en el campo **Confirmar nueva contraseña** y seleccione **Intro**.
3. Lea la notificación y haga clic en **sí** para aceptar el cambio.
4. Espere la confirmación del cambio y seleccione **Cerrar**.
5. Para aplicar los cambios, debe reiniciar los servicios del servidor de gestión.
6. Después del reinicio, asegúrese de que el servidor de gestión se está ejecutando.

Quitar la protección por contraseña

Si no necesita la protección con contraseña, puede elegir no utilizarla:

1. Seleccione la casilla de verificación: **Elijo no utilizar una contraseña de configuración del sistema y entiendo que la configuración del sistema no será cifrada** y hago clic en **Intro**.
2. Lea la notificación y haga clic en **sí** para aceptar el cambio.
3. Espere la confirmación del cambio y seleccione **Cerrar**.
4. Para aplicar los cambios, debe reiniciar los servicios del servidor de gestión.
5. Después del reinicio, asegúrese de que el servidor de gestión se está ejecutando.

Introducir los ajustes de la contraseña de configuración del sistema (recuperación)

Si el archivo que contiene la configuración de la contraseña se borra debido a un fallo de hardware o a otras razones, tendrá que proporcionar la configuración de la contraseña del sistema para acceder a la base de datos que contiene la configuración del sistema. Durante la instalación en su nuevo ordenador, se le pedirá que introduzca la contraseña de configuración del sistema.

Pero si el archivo que contiene la configuración de la contraseña se ha borrado o corrompido, y el ordenador que está ejecutando el servidor de gestión no tiene ningún otro problema, tiene la opción de introducir los ajustes de la contraseña de configuración del sistema:

1. Localice el icono de la bandeja del servidor de gestión.
2. Haga clic con el botón derecho en el icono de servicio del área de notificación de Management Server y seleccione **Introducir la contraseña de configuración del sistema**.
3. Aparece la ventana de ajustes de la contraseña de configuración del sistema.

La configuración del sistema está protegida por contraseña

1. Escriba la contraseña en el campo de la **contraseña** y seleccione **Intro**.
2. Espere a que la contraseña sea aceptada. Seleccione **Cerrar**.
3. Asegúrese de que el servidor de gestión está en ejecución.

La configuración del sistema no está protegida por contraseña

1. Seleccione la casilla de verificación: **Este sistema no utiliza una contraseña de configuración del sistema** y seleccione **Intro**.
2. Espere a que se acepte el ajuste. Seleccione **Cerrar**.
3. Asegúrese de que el servidor de gestión está en ejecución.

Manually backing up your system configuration (explicación)

Cuando quiera realizar una copia de seguridad manual de la base de datos SQL del servidor de gestión que contiene la configuración de su sistema, asegúrese de que su sistema permanece en línea. El nombre por defecto de la base de datos SQL del servidor de gestión es **Surveillance**.

Aquí hay algunas cosas que hay que tener en cuenta antes de iniciar la copia de seguridad:

- No se puede utilizar una copia de seguridad de la base de datos SQL para copiar las configuraciones del sistema a otros sistemas
- La copia de seguridad de la base de datos SQL puede llevar algún tiempo. Depende de la configuración de su sistema, de su hardware y de si su SQL Server, servidor de gestión y Management Client están instalados en el mismo ordenador
- Los registros, incluidos los de auditoría, se almacenan en la base de datos SQL del servidor de registros y, por tanto, **no** forman parte de una copia de seguridad de la base de datos SQL del servidor de gestión. El nombre por defecto de la base de datos SQL del servidor de registro es **SurveillanceLogServerV2**. Hace una copia de seguridad de ambas bases de datos SQL de la misma manera.

Hacer una copia de seguridad y restaurar la configuración del servidor de eventos (explicación)

El contenido de la configuración del servidor de eventos se incluye cuando se hace una copia de seguridad y se restaura la configuración del sistema.

La primera vez que ejecuta el servidor de eventos, todos sus archivos de configuración se trasladan automáticamente a la base de datos 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 toda la comunicación externa mientras se carga la restauración de la configuración.

Copia de seguridad y restauración programada de la configuración del sistema (explicación)

El servidor de gestión almacena la configuración de su sistema en una base de datos SQL. Milestone recomienda que realice regularmente copias de seguridad programadas de esta base de datos SQL como medida de recuperación de desastres. Aunque es raro perder la configuración del sistema, puede ocurrir en circunstancias desafortunadas. Por suerte, solo se tarda un minuto, y las copias de seguridad también tienen la ventaja añadida de que vacían el registro de transacciones de su base de datos SQL.

Si tiene una configuración más pequeña y no necesita copias de seguridad programadas, puede hacer una copia de seguridad de la configuración del sistema manualmente. Para obtener instrucciones, consulte Manually backing up your system configuration (explicación) en la página 346.

Cuando haga una copia de seguridad/restauración del servidor de gestión, asegúrese de que la base de datos SQL con la configuración del sistema está incluida en la copia de seguridad/restauración.

Requisitos para usar la copia de seguridad y restauración programada

Microsoft® SQL Server Management Studio, una herramienta que se puede descargar gratuitamente desde su sitio web (https://www.microsoft.com/downloads/).

Además de gestionar SQL Server y sus bases de datos, la herramienta incluye algunas funciones de copia de seguridad y restauración fáciles de usar. Descargue e instale la herramienta en su servidor de gestión.

Hacer una copia de seguridad de la configuración del sistema con una copia de seguridad programada

1. En el menú Inicio de Windows, inicie Microsoft® SQL Server Management Studio.
2. Cuando se conecte, especifique el nombre del SQL Server requerido. Utilice la cuenta con la que creó la base de datos SQL.
    1. Encuentre la base de datos SQL que contiene toda la configuración de su sistema, incluyendo el servidor de eventos, los servidores de grabación, las cámaras, las entradas, las salidas, los usuarios, las reglas, los perfiles de patrulla, etc. El nombre por defecto de esta base de datos SQL es **Surveillance**.
    2. Haga una copia de seguridad de la base de datos SQL y asegúrese de:
        - Verificar que la base de datos SQL seleccionada es la correcta
        - Verificar que el tipo de copia de seguridad es **completa**
        - Establezca la programación de la copia de seguridad recurrente. Puede leer más sobre las copias de seguridad programadas y automatizadas en el sitio web de Microsoft (https://docs.microsoft.com/en-us/sql/relational-databases/logs/the-transaction-log-sql-server?view=sql-server-2017
        - Verificar que la ruta sugerida es satisfactoria o seleccionar una ruta alternativa
        - Seleccione que se **verifique la copia de seguridad al terminar** y que se **realice la suma de comprobación antes de escribir en los medios**
3. Siga las instrucciones de la herramienta hasta el final.

Considere también la posibilidad de hacer una copia de seguridad de la base de datos SQL del servidor de registro con sus registros utilizando el mismo método. El nombre por defecto de la base de datos SQL del servidor de registro es **SurveillanceLogServerV2**.

Restaurar la configuración del sistema a partir de una copia de seguridad programada

Requisitos
Para evitar que se realicen cambios en la configuración del sistema mientras se restaura la base de datos SQL de configuración del sistema, detenga el:

- Management Server servicio (consulte Gestión de los servicios del servidor en la página 362)
- Event Server servicio (puede hacerse desde **Servicios** de Windows (busque **services.msc** en su máquina. Dentro de **Servicios**, ubique **Milestone XProtect Event Server**))
- Servicio de publicación en la World Wide Web, también conocido como Servicio de Información de Internet (IIS). Aprenda a detener el IIS (https://technet.microsoft.com/library/cc732317(WS.10).aspx/)

Abrir Microsoft® SQL Server Management Studio desde el menú **Inicio** de Windows.

En la herramienta haga lo siguiente:

1. Cuando se conecte, especifique el nombre del SQL Server requerido. Utilice la cuenta de usuario con la que se creó la base de datos SQL.
2. Encuentre la base de datos SQL (el nombre por defecto es **Surveillance**) que contiene toda la configuración de su sistema, incluyendo el servidor de eventos, los servidores de grabación, las cámaras, las entradas, las salidas, los usuarios, las reglas, los perfiles de patrulla, etc.
3. Haga una restauración de la base de datos SQL y asegúrese de:
   - Seleccionar hacer una copia de seguridad **desde** el dispositivo
   - Seleccionar el **archivo** del tipo de medios de copia de seguridad
   - Encontrar y seleccionar el archivo de copia de seguridad (**.bak**)
   - Seleccionar **sobrescribir la base de datos existente**
4. Siga las instrucciones de la herramienta hasta el final.

Use el mismo método para restaurar la base de datos SQL del servidor de registro con sus registros. El nombre por defecto de la base de datos SQL del servidor de registro es **SurveillanceLogServerV2**.

> El sistema no funciona mientras el servicio Management Server está detenido. Es importante recordar que hay que volver a iniciar todos los servicios una vez que se haya terminado de restaurar la base de datos.

Copia de seguridad de la base de datos SQL del servidor de registro

Maneje la base de datos SQL del servidor de registro usando el método que utiliza cuando maneja la configuración del sistema como se describió anteriormente. La base de datos SQL del servidor de registro contiene todos los registros del sistema, incluidos los errores notificados por los servidores de grabación y las cámaras. El nombre por defecto de la base de datos SQL del servidor de registro es **SurveillanceLogServerV2**.

La base de datos SQL se encuentra en el servidor de registro SQL Server. Normalmente, el servidor de registro y el servidor de gestión tienen sus bases de datos SQL en el mismo SQL Server. Hacer una copia de seguridad de la base de datos SQL del servidor de registro no es vital, ya que no contiene ninguna configuración del sistema, pero puede apreciar tener acceso a los registros del sistema desde antes de la copia de seguridad/restauración del servidor de gestión.

Escenarios de fallos y problemas de copia de seguridad y restauración (explicación)

- Si, después de la última copia de seguridad de la configuración del sistema, ha trasladado el servidor de eventos u otros servicios registrados, como el servidor de registros, debe seleccionar qué configuración de servicios registrados desea para el nuevo sistema. Puede decidir mantener la nueva configuración después de restaurar el sistema a la versión anterior. Decide mirando 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 antigua configuración del servicio registrado), realice otra restauración.
- Si está restaurando una copia de seguridad de la configuración e introduce una contraseña de configuración del sistema que es incorrecta, debe proporcionar la contraseña de configuración del sistema que era válida en el momento en que se creó la copia de seguridad.

Mover el servidor de gestión

El servidor de gestión almacena la configuración de su sistema en una base de datos SQL. Si va a trasladar el servidor de gestión de un servidor físico a otro, es vital que tenga la certeza de que su nuevo servidor de gestión también tiene acceso a esta base de datos SQL. La base de datos SQL de configuración del sistema puede almacenarse de dos maneras diferentes:

- **Red SQL Server**: Si almacena la configuración de su sistema en una base de datos SQL en una SQL Server en su red, puede apuntar a la ubicación de la base de datos SQL en esa SQL Server al instalar el software del servidor de gestión en su nuevo servidor de gestión. En ese caso, solo se aplica el siguiente párrafo sobre el nombre del servidor de gestión y la dirección IP y debe ignorar el resto de este tema:

  Nombre del host del servidor de gestión y dirección IP: Cuando se traslada el servidor de gestión de un servidor físico a otro, lo más fácil es dar al nuevo servidor el mismo nombre de host y la misma dirección IP que el anterior. Esto se debe a que el servidor de grabación se conecta automáticamente al nombre de host y a la dirección IP del antiguo servidor de gestión. Si le da al nuevo servidor de gestión un nuevo nombre de host y/o dirección IP, el servidor de grabación no podrá encontrar el servidor de gestión y deberá detener manualmente cada servicio Recording Server en su sistema, cambiar la URL de su servidor de gestión, registrar de nuevo el servidor de grabación y, una vez hecho esto, iniciar el servicio Recording Server.
- **Local SQL Server**: Si almacena la configuración del sistema en una base de datos SQL en un SQL Server en el propio servidor de gestión, es importante que haga una copia de seguridad de la base de datos SQL de configuración del sistema del servidor de gestión existente antes del traslado. Haciendo una copia de seguridad de la base de datos SQL y restaurándola posteriormente en un SQL Server en el nuevo servidor de gestión, evitará tener que reconfigurar sus cámaras, reglas, perfiles temporales, etc. después del traslado

Si traslada el servidor de gestión, necesitará la contraseña de configuración actual del sistema para poder restaurar la copia de seguridad, consulte Contraseña de configuración del sistema (explicación) en la página 343.

Requisitos

- **Su 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 debe utilizar el archivo de licencia de software activado 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 puede reutilizarse cuando se traslada a un nuevo servidor

Si también está actualizando el software de su sistema en relación con el traslado, ha recibido un nuevo archivo de licencia de software. Simplemente utilice esto.

- **Solo usuarios locales SQL Server: Microsoft® SQL Server Management Studio**
- ¿Qué ocurre mientras el servidor de gestión no está disponible? Unavailable management servers (explicación) en la página 350)
- Copiar la base de datos del servidor de registro (consulte Copia de seguridad de la base de datos SQL del servidor de registro en la página 348)

Unavailable management servers (explicación)

- **Los servidores de grabación pueden seguir grabando**: Todos los servidores de grabación en funcionamiento han recibido una copia de su configuración desde el servidor de gestión, por lo que pueden trabajar y almacenar grabaciones por su cuenta mientras el servidor de gestión está inactivo. Por lo tanto, la grabación programada y activada por movimiento funciona, y la grabación activada por eventos funciona a menos que se base en eventos relacionados con el servidor de gestión o cualquier otro servidor de grabación, ya que éstos pasan por el servidor de gestión
- **Los servidores de grabación almacenan temporalmente los datos de registro a nivel local**: Envían automáticamente los datos de registro al servidor de gestión cuando vuelve a estar disponible:
    - **Los clientes no pueden iniciar sesión**: El acceso de los clientes se autoriza a través del servidor de gestión. Sin el servidor de gestión, los clientes no pueden iniciar sesión
    - **Los clientes que ya han iniciado sesión pueden permanecer conectados hasta cuatro horas**: Cuando los clientes inician sesión, son autorizados por el servidor de gestión y pueden comunicarse con los servidores de grabación durante un máximo de cuatro horas. Si puede poner en marcha el nuevo servidor de gestión en cuatro horas, muchos de sus usuarios no se verán afectados
    - **No se puede configurar el sistema**: Sin el servidor de gestión, no puede cambiar la configuración del sistema

Milestone recomienda que informe a sus usuarios sobre el riesgo de perder el contacto con el sistema de vigilancia mientras el servidor de gestión esté inactivo.

Mover la configuración del sistema

Mover la configuración del sistema es un proceso de tres pasos:

1. Haga una copia de seguridad de la configuración de su sistema. Esto es idéntico a realizar una copia de seguridad programada. Consulte también Hacer una copia de seguridad de la configuración del sistema con una copia de seguridad programada en la página 347.
2. Instale el nuevo servidor de gestión en el nuevo servidor. Consulte la copia de seguridad programada, paso 2.
3. Restaurar la configuración del sistema en el nuevo sistema. Consulte también Restaurar la configuración del sistema a partir de una copia de seguridad programada en la página 347.

Sustituir un servidor de grabación

Si un servidor de grabación funciona mal y quiere sustituirlo por un nuevo servidor que herede la configuración del antiguo servidor de grabación:

1. Recupere el ID del servidor de grabación del antiguo servidor de grabación:
    1. Seleccione **Servidores de grabación** y, a continuación, en el panel **Generalidades** seleccione el antiguo servidor de grabación.
    2. Seleccione la pestaña **Almacenamiento**.
    3. Mantenga pulsada la tecla CTRL de su teclado mientras selecciona la pestaña **Información**.
    4. Copie el número de ID del servidor de grabación en la parte inferior de la pestaña de **Información**. No copie el término *ID*, solo el número en sí.

2. Sustituya el ID del servidor de grabación en el nuevo servidor de grabación:
    1. Detenga el servicio Recording Server en el antiguo servidor de grabación y, a continuación, en los **Servicios** de Windows, establezca el **Tipo de inicio** del servicio en **Deshabilitado**.

> **!** Es muy importante que no inicie dos servidores de grabación con identificaciones idénticas al mismo tiempo.

2. En el nuevo servidor de grabación, abra un explorador y diríjase a `C:\ProgramData\Milestone\XProtect Servidor de grabación` o a la ruta donde se encuentre su servidor de grabación.
3. Abra el archivo `RecorderConfig.xml`.
4. Elimine el ID indicado entre las etiquetas *<id>* y *</id>*.

5. Pegue el ID del servidor de grabación copiado entre las etiquetas *<id>* e *</id>*. Guarde el archivo *RecorderConfig.xml*.
6. Vaya al registro: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\VideoOS\Recorder\Installation`.
7. Abra **RecorderIDOnMachine** y cambie el antiguo ID del servidor de grabación por el nuevo ID.

3. Registre el nuevo servidor de grabación en el servidor de gestión. Para ello, haga clic con el botón derecho del ratón en el icono de la bandeja Recording Server Manager y haga clic en **Registrar**. Si desea más información, consulte Registrar un servidor de grabación en la página 199.
4. Reinicie el servicio Recording Server. Cuando el nuevo servicio Recording Server se pone en marcha, ha heredado todos los ajustes del antiguo servidor de grabación.

Mover el hardware

Puede mover el hardware entre los servidores de grabación que pertenecen al mismo sitio. Después de un traslado, el hardware y sus dispositivos funcionan en el nuevo servidor de grabación y las nuevas grabaciones se almacenan en este servidor. El movimiento es transparente para los usuarios clientes.

Las grabaciones en el antiguo servidor de grabación permanecen allí hasta que:

- El sistema los borra cuando el tiempo de retención expira. Las grabaciones que alguien ha protegido con el Bloqueo de evidencias (consulte Bloqueos de evidencias (explicación) en la página 75) no se eliminan hasta que expira el tiempo de retención del bloqueo de evidencias. Define el tiempo de retención de los bloqueos de pruebas cuando los crea. El tiempo de retención potencialmente nunca expira
- Las elimina desde cada servidor de grabación nuevo del dispositivo en la pestaña **Grabar**

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

> Si mueve el hardware a un servidor de grabación que actualmente no tiene hardware añadido, los usuarios del cliente deben cerrar la sesión e iniciarla para recibir los datos de los dispositivos.

Puede utilizar la función de mover el hardware para:

- **Balance de carga**: Si, por ejemplo, el disco de un servidor de grabación está sobrecargado, puede añadir un nuevo servidor de grabación y mover parte de su hardware
- **Actualizar**: Si, por ejemplo, el disco de un servidor de grabación está sobrecargado, puede añadir un nuevo servidor de grabación y mover parte de su hardware
- **Sustituir un servidor de grabación defectuoso**: Si, por ejemplo, el servidor está desconectado y no va a volver a conectarse, puede trasladar el hardware a otros servidores de grabación y así mantener el sistema en funcionamiento. No puede acceder a las grabaciones antiguas. Si desea más información, consulte Sustituir un servidor de grabación en la página 351.

Grabaciones a distancia

Cuando se mueve el hardware a otro servidor de grabación, el sistema cancela las recuperaciones en curso o programadas de los sitios interconectados o de los almacenamientos de borde de las cámaras. Las grabaciones no se borran, pero los datos no se recuperan ni se guardan en las bases de datos como se esperaba. Si este es el caso, recibirá una advertencia. Para el usuario XProtect Smart Client, que ha iniciado una recuperación cuando se inicia el traslado del hardware, la recuperación falla. El usuario de XProtect Smart Client recibe una notificación y puede volver a intentarlo más tarde.

Si alguien ha movido el 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 lo sincroniza, las cámaras desplazadas permanecen desconectadas en el sitio central.

Mover el hardware (asistente)

Para mover el hardware de un servidor de grabación a otro, ejecute el asistente para **Mover hardware**. El asistente le guiará a través de los pasos necesarios para completar un traslado 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 física a través de la red
- Instale un servidor de grabación al que desee trasladar el hardware (consulte Instalación a través de Download Manager (explicación) en la página 170 o Instalar un servidor de grabación de forma silenciosa en la página 179)
- Instale en el nuevo servidor de grabación las mismas versiones de paquetes de dispositivos que ejecuta en el servidor existente (consulte Controladores de dispositivos (explicación) en la página 149)

Para ejecutar el asistente:

1. En el panel **Navegación del sitio**, seleccione **Servidores de grabación**.
2. En el panel de **Generalidades**, haga clic con el botón derecho en el servidor de grabación del que desea mover el hardware o haga clic con el botón derecho en un dispositivo de hardware específico.

3. Seleccione **Mover hardware**.

   > Si el servidor de grabación desde el que se mueve el hardware está desconectado, aparece un mensaje de error. Solo debe optar por trasladar el hardware de un servidor de grabación desconectado si tiene la certeza de que no volverá a conectarse. Si traslada el hardware de todos modos y el servidor vuelve a estar en línea, se arriesga a que el sistema tenga un comportamiento inesperado por tener el mismo hardware funcionando en dos servidores de grabación durante un período. Los 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, aparecerá la página **Seleccionar el hardware que desea mover**. Seleccione los dispositivos de hardware que desea mover.
5. En la página **Seleccionar el servidor de grabación al que desea mover el hardware**, seleccione de la lista de servidores de grabación instalados en este sitio.
6. En la página **Seleccionar el almacenamiento que desea utilizar para grabaciones futuras**, la barra de uso del almacenamiento indica el espacio libre en la base de datos de grabaciones solo para las grabaciones en directo, no para los archivos. El tiempo de retención total es el periodo de retención tanto de la base de datos de registro como de los archivos.
7. El sistema procesa su solicitud.
8. Si el movimiento fue exitoso, haga clic en **Cerrar**. Si selecciona el nuevo servidor de grabación en el Management Client, puede ver el hardware trasladado y ahora las grabaciones se almacenan en este servidor.

   Si el movimiento falló, puede solucionar el problema más abajo.

   > En un sistema interconectado, debe sincronizar manualmente el sitio central después de mover el hardware en un sitio remoto para reflejar los cambios que usted, u otro administrador del sistema, hizo en el sitio remoto.

Solución de problemas al mover el hardware

Si un movimiento no tuvo éxito, uno de los siguientes motivos puede ser la causa:

Tipo de error	Solución de problemas
El servidor de grabación no está	Asegúrese de que el servidor de grabación está en línea. Es

Tipo de error	Solución de problemas
conectado o está en modo failover.	posible que tenga que registrarlo. Si el servidor está en modo failover, espere y vuelva a intentarlo.
El servidor de grabación no es la última versión.	Actualice el servidor de grabación para que ejecute la misma versión que el servidor de gestión.
No se ha podido encontrar el servidor de grabación en la configuración.	Asegúrese de que el servidor de grabación no ha sido eliminado.
Ha fallado la actualización de la configuración o la comunicación con la base de datos de configuración.	Asegúrese de que su SQL Server y la base de datos están conectadas y funcionando.
Se ha producido un error en el servidor de grabación actual	Es posible que otro proceso haya bloqueado el servidor de grabación, o que el servidor de grabación esté en modo de error. Asegúrese de que el servidor de grabación está funcionando y vuelva a intentarlo.
El hardware no existe.	Asegúrese de que el hardware que intenta mover no ha sido eliminado simultáneamente del sistema por otro usuario. El escenario es bastante improbable.
El servidor de grabación del que se movió el hardware vuelve a estar en línea, pero eligió ignorarlo cuando estaba desconectado.	Lo más probable es que haya aceptado que el antiguo servidor de grabación no volverá a estar en línea cuando inició el asistente para **Mover hardware**, pero durante el traslado, el servidor se conectó. Inicie de nuevo el asistente y seleccione **No** cuando se le pida que confirme si el servidor vuelve a estar en línea.
El almacenamiento de grabación de la fuente no está disponible.	Está intentando mover el hardware con dispositivos configurados con un almacenamiento de grabación que actualmente está desconectado. Un almacenamiento de grabación está fuera de línea si el disco está desconectado o no está disponible.

Tipo de error	Solución de problemas
	Asegúrese de que el almacenamiento de la grabación está en línea y vuelva a intentarlo.
Todos los almacenamientos de grabación en el servidor de grabación de destino deben estar disponibles.	Está intentando mover el hardware a un servidor de grabación en el que uno o más almacenamientos de grabación están actualmente desconectados. Asegúrese de que todos los almacenamientos de grabación en el servidor de grabación de destino están en línea. Un almacenamiento de grabación está fuera de línea si el disco está desconectado o no está disponible.

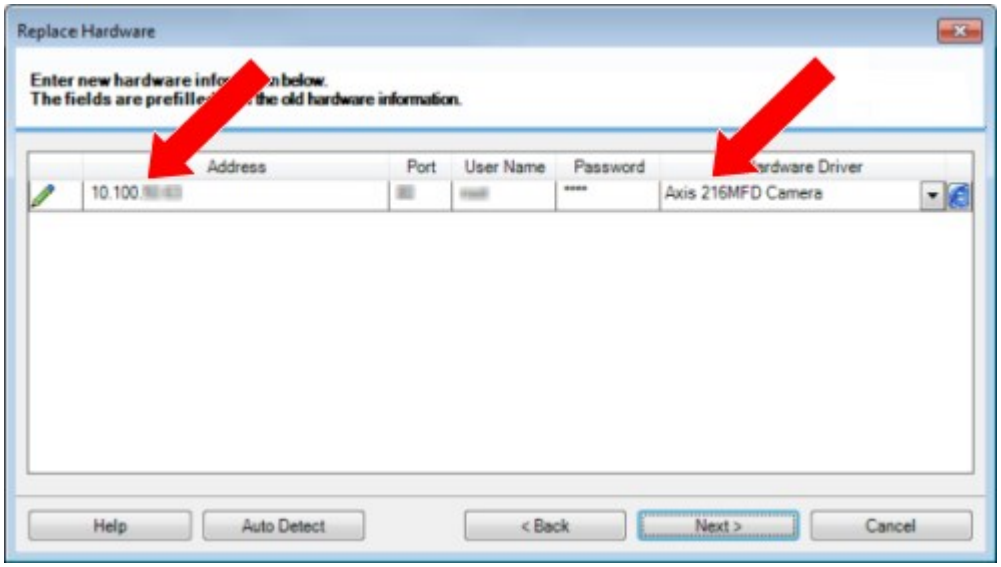
Sustituir el hardware

Cuando sustituya un dispositivo de hardware en su red por otro dispositivo de hardware, debe conocer la dirección IP, el puerto, el nombre de usuario y la contraseña del nuevo dispositivo de hardware.

Si no ha habilitado la activación automática de las licencias (consulte Activación de licencia automática (explicación) en la página 119 y ha utilizado todos los cambios de dispositivos sin activación (consulte Cambios en el dispositivo sin activación (explicación) en la página 120), deberá activar manualmente sus licencias **después** de sustituir los dispositivos de hardware. Si el nuevo número de dispositivos de hardware supera su número total de licencias de dispositivos, tendrá que adquirir nuevas licencias de dispositivos.

1. Expanda el servidor de grabación requerido, haga clic con el botón derecho del ratón en el hardware que desea sustituir.
2. Seleccione **Reemplazar hardware**.
3. Aparece el asistente **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 lo conoce, seleccione el driver correspondiente en la lista desplegable del **Driver de hardware**. De lo contrario, seleccione **Detección automática**. Si los datos del puerto, el nombre de usuario o la contraseña son diferentes para el nuevo hardware, corríjalos **antes de iniciar el proceso de detección automática (si es necesario)**.



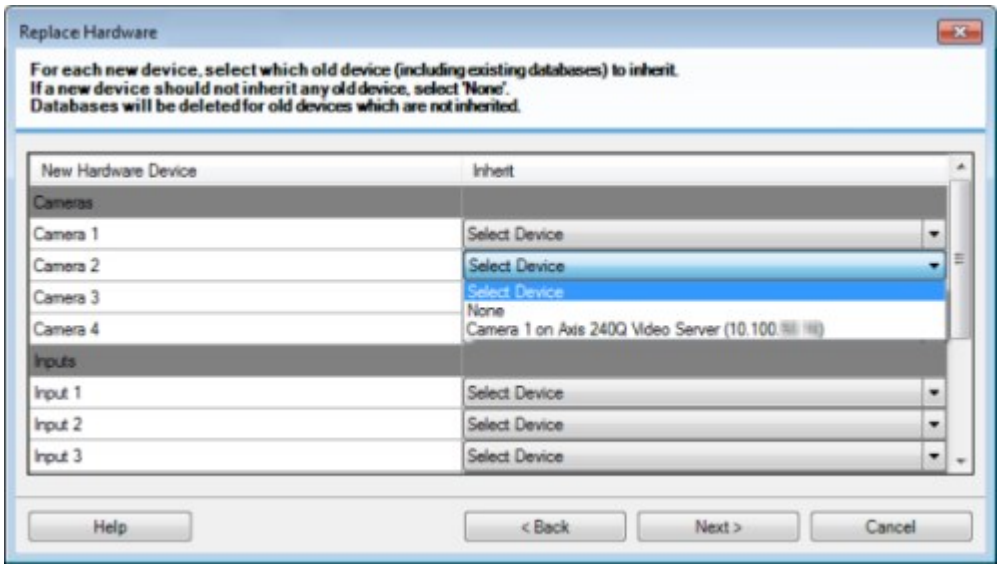
El asistente se rellena previamente con los datos del hardware existente. Si lo sustituye por un dispositivo de hardware similar, puede reutilizar algunos de estos datos, por ejemplo, la información del puerto y del controlador.

5. Haga una de las siguientes cosas:
   - Si ha seleccionado el controlador de dispositivo de hardware necesario directamente de la lista, haga clic en **Siguiente**
   - Si ha seleccionado **Detección automática** en la lista, haga clic en **Detección automática**, espere a que este proceso tenga éxito (marcado con una ✓ en el extremo izquierdo), haga clic en **Siguiente**

     Este paso está diseñado para ayudarle a planificar los dispositivos y sus bases de datos, en función del número de cámaras individuales, micrófonos, entradas, salidas, etc. conectados al dispositivo de hardware antiguo y al nuevo respectivamente.

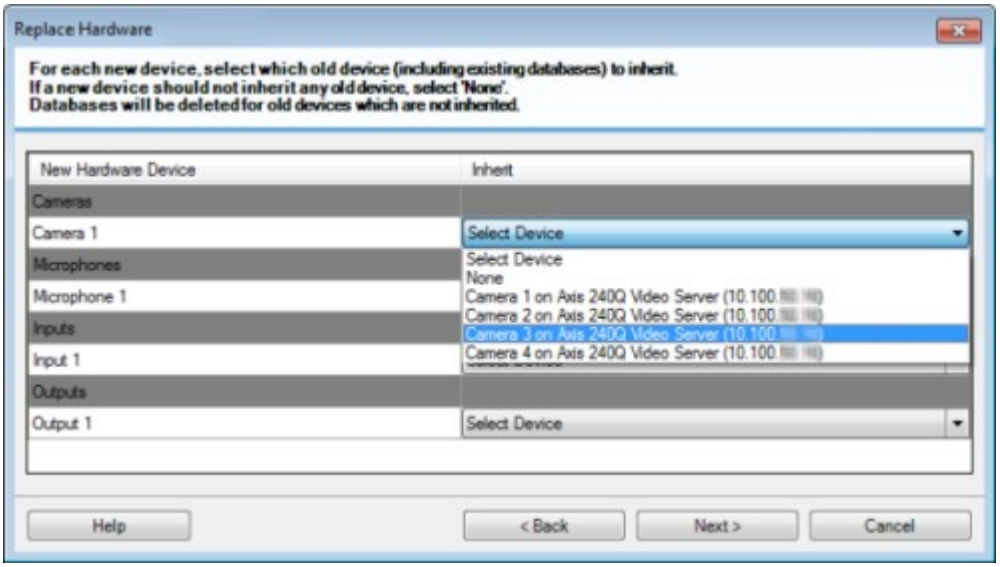
     Es importante tener en cuenta **cómo** asignar las bases de datos del dispositivo de hardware antiguo a las bases de datos del nuevo dispositivo de hardware. Realiza la asignación de los dispositivos individuales seleccionando la cámara, el micrófono, la entrada, la salida o **Ninguno** correspondientes en la columna de la derecha.

     > ⚠ Asegúrese de asignar **todas** las cámaras, micrófonos, entradas, salidas, etc. Los contenidos asignados a **Ninguno**, se **pierden**.



Ejemplo de que el dispositivo de hardware antiguo tiene más dispositivos individuales que el

nuevo:



Haga clic en **Siguiente**.

6. Se le presenta una lista de hardware que debe añadirse, sustituirse o eliminarse. Haga clic en **Confirmar**.
7. El último paso es un resumen de los dispositivos añadidos, sustituidos y heredados y sus ajustes. Haga clic en **Copiar en el portapapeles** para copiar el contenido en el portapapeles de Windows o/y en **Cerrar** para finalizar el asistente.

Actualizar los datos de su hardware

Para tener certeza de que su dispositivo de hardware y el sistema están utilizando la misma versión de firmware, debe actualizar manualmente los datos de hardware del dispositivo de hardware en el Management Client. Milestone recomienda que actualice los datos del hardware después de cada actualización del firmware de su dispositivo de hardware.

Para obtener los últimos datos del hardware:

1. En el panel **Navegación del sitio**, seleccione **Servidores de grabación**.
2. Expanda el servidor de grabación requerido y seleccione el hardware del que desea obtener la información más reciente.
3. En el panel **Propiedades** de la pestaña **Información**, haga clic en el botón **Actualizar** en el campo **Datos de hardware actualizados por última vez.**.

4. El asistente comprueba si el sistema está ejecutando el último firmware para el hardware.

   Seleccione **Confirmar** para actualizar la información en el Management Client. Cuando la actualización se ha completado, la versión actual del firmware para el dispositivo de hardware detectado por el sistema aparece en el campo **Versión del firmware** de la pestaña **Información**.

Gestionar el SQL Server y la base de datos

Cambiar el SQL Server y las direcciones de la base de datos (explicación)

Cuando instale un sistema como prueba, o si reestructura una instalación grande, es posible que tenga que utilizar una SQL Server diferente y una base de datos.

Puede cambiar la dirección de SQL Server y de la base de datos utilizada por el servidor de gestión y por el servidor de eventos, y la dirección de SQL Server y de la base de datos utilizadas por el servidor de registro, el servidor de XProtect Incident Manager y el servidor de Identity Provider. La única limitación es que no puede cambiar las direcciones SQL del servidor de gestión y del servidor de eventos al mismo tiempo que la dirección SQL del servidor de registro. Puede hacerlo uno tras otro.

Debe cambiar las direcciones de SQL Server y de base de datos localmente a través del Registro de Windows en los ordenadores donde haya instalado los servidores. Si su servidor de gestión y su servidor de eventos están instalados en ordenadores distintos, deberá actualizar las direcciones en ambos ordenadores.

Debe copiar las bases de datos SQL antes de continuar.

Cambiar el servidor de registro de SQL Server y la base de datos

Para cambiar la ubicación de SQL para el Log Server, haga lo siguiente:

Antes de hacer ningún cambio en el registro, haga una copia de seguridad del registro.

1. Asegúrese de que el usuario que ejecuta el grupo de aplicaciones de Log Server es el propietario (DBO) de la base de datos del servidor de registros.
2. Actualice la cadena de conexión en el Registro de Windows para incluir la nueva ubicación y el nombre del servidor de registro. El valor se puede encontrar y modificar en:

   HKEY_LOCAL_MACHINE\SOFTWARE\VideoOS\Server\ConnectionString:
3. Reinicie el servicio Log Server mediante Servicios Windows.

El nombre de la base de datos por defecto es: *SurveillanceLogServerV2*.

Cambie el servidor de gestión y el servidor de eventos SQL Server y la base de datos.

Para cambiar la ubicación SQL del servidor de gestión y del servidor de eventos, haga lo siguiente:

Antes de hacer ningún cambio en el registro, haga una copia de seguridad del registro.

1. Detenga los servicios y asegúrese de que el usuario que ejecuta el servidor de gestión y el servidor de eventos sea el propietario (DBO) de la base de datos.
2. Actualice la cadena de conexión en el Registro de Windows para incluir la nueva ubicación y el nombre de los servidores. Los valores se pueden encontrar y modificar en:

   HKEY_LOCAL_MACHINE\SOFTWARE\VideoOS\Server\ConnectionString:
3. Reinicie el Management Server y el XProtect Event Server a través de Servicios Windows o desde los iconos de bandeja en el área de notificación.

El nombre de la base de datos por defecto es: *Vigilancia*.

Las cadenas de conexión son: *ManagementServer* y *EventServer*.

Si el servidor de eventos se está ejecutando en un ordenador diferente, haga el mismo cambio allí. El servidor de eventos y el servidor de gestión utilizan la misma base de datos.

Cambie el servidor de registro de XProtect Incident Manager SQL Server y la base de datos

Antes de hacer ningún cambio en el registro, haga una copia de seguridad del registro.

1. Detenga el servicio y asegúrese de que el usuario que ejecuta el servidor XProtect Incident Manager sea el propietario (DBO) de la base de datos.
2. Actualice la cadena de conexión en el Registro de Windows para incluir la nueva ubicación y el nombre del servidor. Los valores se pueden encontrar y modificar en:

   HKEY_LOCAL_MACHINE\SOFTWARE\VideoOS\Server\ConnectionString:
3. Reinicie el Incident Manager desde el Manager IIS.

El nombre de la base de datos por defecto es: *Surveillance_IM*.

Cambiar el servidor de Identity Provider de SQL Server y la base de datos

Antes de hacer ningún cambio en el registro, haga una copia de seguridad del registro.

1. Detenga el servicio y asegúrese de que el usuario que ejecuta el servidor Identity Provider sea el propietario (DBO) de la base de datos.
2. Actualice la cadena de conexión en el Registro de Windows para incluir la nueva ubicación y el nombre del servidor. Los valores se pueden encontrar y modificar en:

   HKEY_LOCAL_MACHINE\SOFTWARE\VideoOS\Server\ConnectionString:
3. Reinicie el OD desde el Manager IIS.

El nombre de la base de datos por defecto es: *Surveillance_IDP*.

Gestión de los servicios del servidor

En el ordenador 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 iconos, puede obtener información sobre los servicios y realizar determinadas tareas. Esto incluye, por ejemplo, comprobar el estado de los servicios, ver los registros o los mensajes de estado, e iniciar y detener los servicios.

Iconos de la bandeja del administrador del servidor (explicación)

Los iconos de bandeja de 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 failover y el servidor de eventos. Son visibles en los ordenadores con los servidores instalados, en el área de notificación:

Management Server Manager icono de bandeja	Recording Server Manager icono de bandeja	Event Server Manager icono de bandeja	Failover Recording Server Manager icono de bandeja	Descripción
				**Ejecutando** Aparece cuando se habilita e inicia un servicio de servidor.

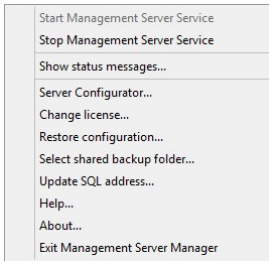
Management Server Manager icono de bandeja	Recording Server Manager icono de bandeja	Event Server Manager icono de bandeja	Failover Recording Server Manager icono de bandeja	Descripción
				Si el servicio Failover Recording Server está funcionando, puede hacerse cargo si los servidores de grabación estándar fallan.
				**Detenido** Aparece cuando un servicio del servidor se ha detenido. Si el servicio Failover Recording Server se detiene, no puede hacerse cargo si los servidores de grabación estándar fallan.

Management Server Manager icono de bandeja	Recording Server Manager icono de bandeja	Event Server Manager icono de bandeja	Failover Recording Server Manager icono de bandeja	Descripción
				**Iniciando** Aparece cuando un servicio del servidor está en proceso de iniciarse. En circunstancias normales, el icono de la bandeja cambia al poco tiempo a **En ejecución**.
				**Deteniéndose** Aparece cuando un servicio del servidor está en proceso de detenerse. En circunstancias normales, el icono de la bandeja cambia al poco tiempo a **Detenido**.
				**En estado indeterminado** Aparece cuando el servicio del servidor se carga inicialmente y hasta que se recibe la primera información, tras lo cual el icono de la bandeja, en circunstancias normales, cambia a **Iniciando** y después a **En ejecución**.
				**Funcionamiento fuera de línea** Suele aparecer cuando el servidor de grabación o el servicio de grabación de failover está en funcionamiento pero el servicio Management Server no lo está.

Iniciar o detener el servicio Management Server

El icono de la bandeja Management Server Manager indica el estado del servicio Management Server, por ejemplo, **En ejecución**. A través de este icono, puede iniciar o detener el servicio Management Server. Si detiene el servicio Management Server, no se podrá utilizar el Management Client.

1. En el área de notificación, haga clic con el botón derecho en el icono de la bandeja Management Server Manager. Aparece un menú contextual.



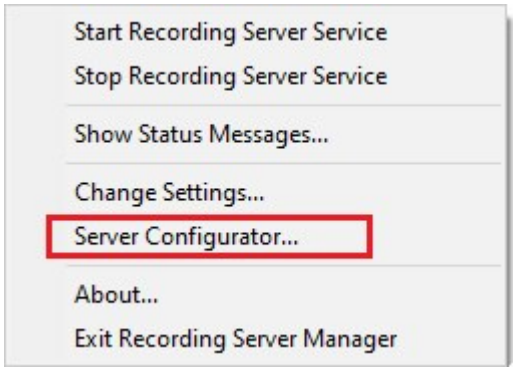
2. Si el servicio se ha detenido, haga clic en **Iniciar servicio Management Server** para iniciarlo. El icono de la bandeja cambia para reflejar el nuevo estado.
3. Para detener el servicio, haga clic en **Detener servicio Management Server**.

> Para obtener más información sobre los iconos de la bandeja, consulte Iconos de la bandeja del administrador del servidor (explicación) en la página 362.

Iniciar o detener el servicio Recording Server

El icono de la bandeja Recording Server Manager indica el estado del servicio Recording Server, por ejemplo, **En ejecución**. A través de este icono, puede iniciar o detener el servicio Recording Server. Si detiene el servicio Recording Server, el sistema no podrá interactuar con los dispositivos conectados al servidor. Esto significa que no puede ver el vídeo en directo ni grabarlo.

1. En el área de notificación, haga clic con el botón derecho en el icono de la bandeja Recording Server Manager. Aparece un menú contextual.

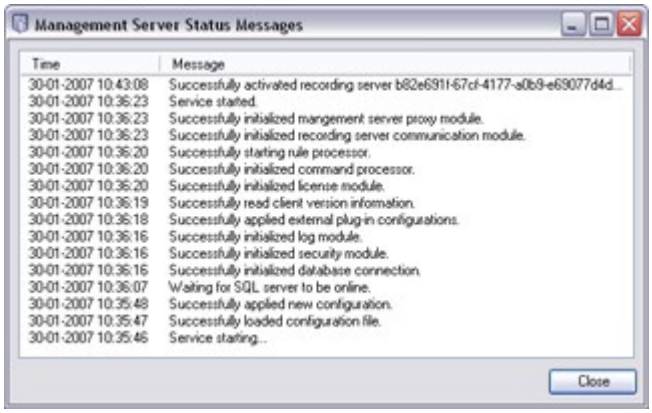


2. Si el servicio se ha detenido, haga clic en **Iniciar servicio Recording Server** para iniciarlo. El icono de la bandeja cambia para reflejar el nuevo estado.
3. Para detener el servicio, haga clic en **Detener servicio Recording Server**.

> Para obtener más información sobre los iconos de la bandeja, consulte Iconos de la bandeja del administrador del servidor (explicación) en la página 362.

Ver los mensajes de estado del Servidor de gestión o del Servidor de grabación

1. En el área de notificación, haga clic con el botón derecho en el icono de la bandeja correspondiente. Aparece un menú contextual.
2. Seleccione **Mostrar mensajes de estado**. Dependiendo del tipo de servidor, aparecerá la ventana de **Mensajes de estado del servidor de gestión** o la de **Mensajes de estado del servidor de grabación**, con una lista de mensajes de estado con marca de tiempo:



Gestionar el cifrado con el Server Configurator

Utilice el Server Configurator para seleccionar los certificados en los servidores locales para la comunicación cifrada y registrar los servicios del servidor para que estén calificados para comunicarse con los servidores.

Abra el Server Configurator desde el menú de inicio de Windows, desde el icono de la bandeja del servidor de gestión o desde el icono de la bandeja del servidor de grabación. Consulte Server Configurator (Utilidad) en la página 418.

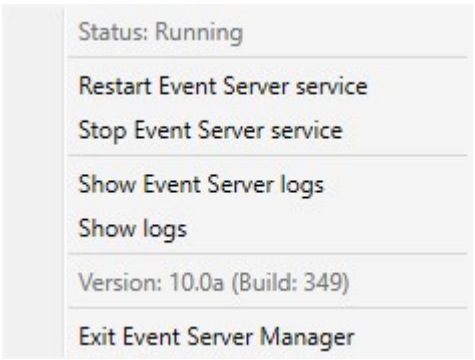
Si desea más información, consulte la guía de certificados sobre cómo asegurar sus instalaciones XProtect VMS.

Iniciar, detener o reiniciar el servicio Event Server

El icono de la bandeja Event Server Manager indica el estado del servicio Event Server, por ejemplo, **En ejecución**. A través de este icono, puede iniciar, detener o reiniciar el servicio Event Server. Si detiene el

servicio, algunas partes del sistema no funcionarán, incluidos los eventos y las alarmas. No obstante, puede seguir viendo y grabando vídeo. Si desea más información, consulte Detener el servicio Event Server en la página 367.

1. En el área de notificación, haga clic con el botón derecho en el icono de la bandeja Event Server Manager. Aparece un menú contextual.



2. Si el servicio se ha detenido, haga clic en **Iniciar servicio Event Server** para iniciarlo. El icono de la bandeja cambia para reflejar el nuevo estado.
3. Para reiniciar o detener el servicio, haga clic en **Reiniciar servicio Event Server** o **Detener servicio Event Server**.

> Para obtener más información sobre los iconos de la bandeja, consulte Iconos de la bandeja del administrador del servidor (explicación) en la página 362.

Detener el servicio Event Server

Cuando se instalan plug-ins de MIP en el Servidor de eventos, primero hay que detener el servicio Event Server y, después, reiniciarlo. Mientras el servicio está detenido, muchas áreas del sistema VMS no funcionarán:

- No se almacenan eventos o alarmas en el Servidor de eventos. No obstante, los eventos del sistema y del dispositivo siguen activando acciones, por ejemplo, iniciar la grabación
- Los productos add-on no funcionan en XProtect Smart Client y no pueden ser configurados desde el Management Client.
- Los eventos analíticos no funcionan
- Los eventos genéricos no funcionan
- No se activa ninguna alarma
- En XProtect Smart Client, los elementos de la vista de plano, los elementos de la vista de lista de

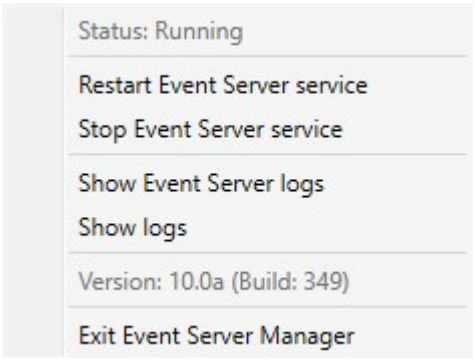
alarmas y el espacio de trabajo del gestor de alarmas no funcionan

- MIP los plug-in en el Servidor de eventos no pueden ejecutarse
- MIP plug-ins en Management Client y XProtect Smart Client no funcionan correctamente

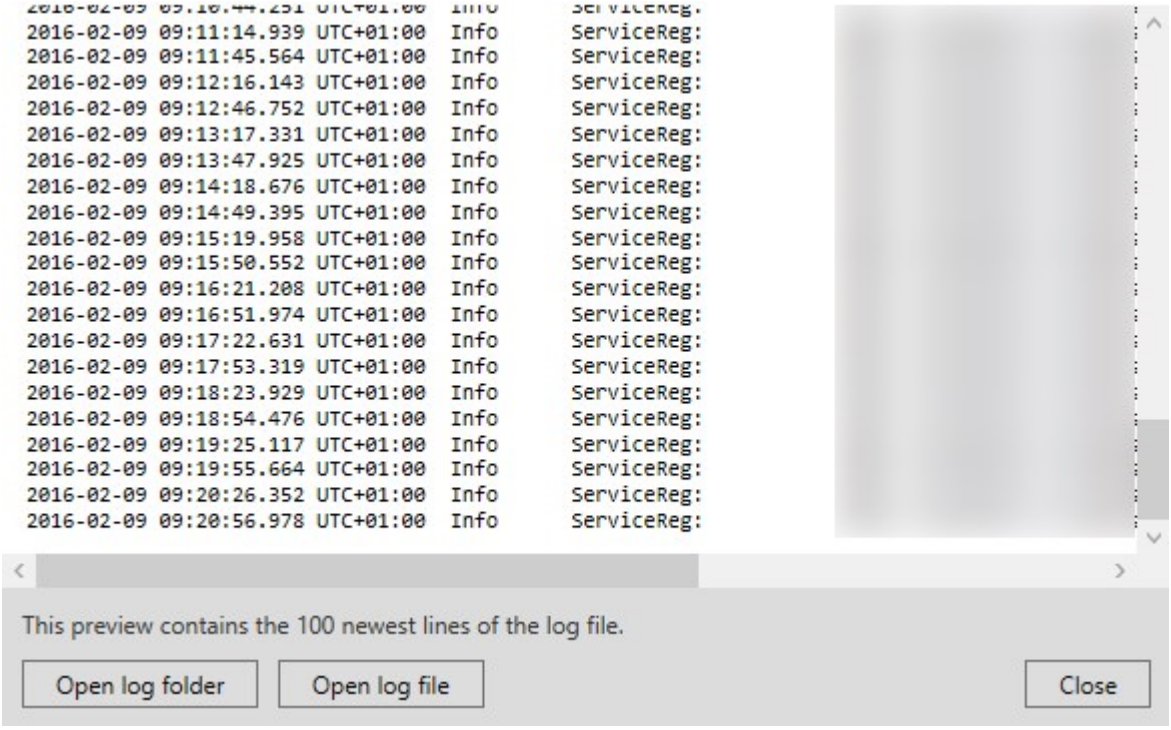
Ver Servidor de eventos o MIP registros

Puede ver la información con marca de tiempo sobre las actividades del Servidor de eventos en el registro del Servidor de eventos. La información sobre las integraciones de terceros se registra en el registro MIP en una subcarpeta de la carpeta del **Servidor de eventos**.

1. En el área de notificación, haga clic con el botón derecho en el icono de la bandeja Event Server Manager. Aparece un menú contextual.



2. Para ver las 100 líneas más recientes del registro de Event Server, haga clic en **Mostrar registros del servidor de eventos**. 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 del registro MIP, vuelva al menú contextual y haga clic en **Mostrar registros MIP**. Se muestra un visor de registro.

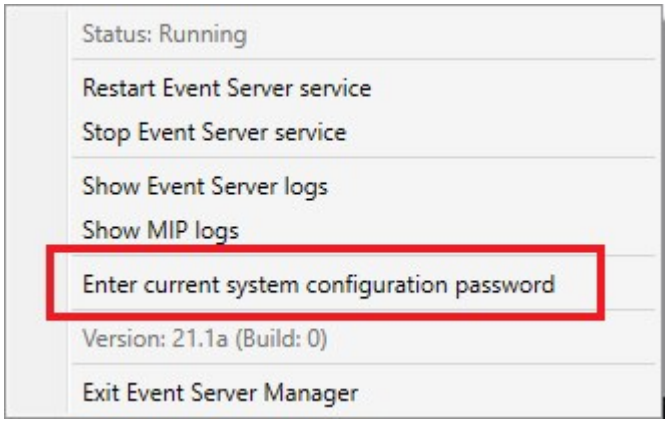
> Si alguien elimina el archivo de registro del directorio de registro, los elementos del menú aparecen en gris. Para abrir el visor de registros, primero hay que copiar el archivo de registro en su carpeta: `C:\ProgramData\Milestone\XProtect Event Server\logs` o `C:\ProgramData\Milestone\XProtect Event Server\logs\MIPRegistros`.

Introduzca la contraseña actual de configuración del sistema

Si la contraseña de configuración del sistema ha sido modificada en el servidor de gestión, deberá introducir también la contraseña de configuración del sistema actual en el servidor de eventos.

> ⚠ Si no se introduce la contraseña actual en el servidor de eventos, los componentes del sistema, como el control de acceso, dejarán de funcionar.

1. En el área de notificación, haga clic con el botón derecho en el icono de la bandeja Event Server Manager. Aparece un menú contextual.



2. Para introducir la contraseña de configuración actual del sistema, haga clic en **Introducir la contraseña de configuración actual del sistema**. Se muestra una ventana.
3. Introduzca la misma contraseña de configuración del sistema que se ha introducido en el servidor de gestión.

Gestión de los servicios registrados

Ocasionalmente, tiene servidores y/o servicios que deben ser capaces de comunicarse con el sistema aunque no formen parte directamente del mismo. Algunos servicios, pero no todos, pueden registrarse automáticamente en el sistema. Los servicios que se pueden registrar automáticamente son:

- Event Server servicio
- Log Server servicio

Los servicios registrados automáticamente aparecen en la lista de servicios registrados.

Puede especificar manualmente los servidores/servicios como servicios registrados en el Management Client.

Añadir y editar servicios registrados

1. En la ventana de **Añadir/Quitar servicios registrados**, haga clic en **Añadir** o **Editar**, según sus necesidades.
2. En la ventana de **Añadir servicio registrado** o **Editar servicio registrado** (dependiendo de su selección anterior), especifique o edite la configuración.
3. Haga clic en **Aceptar**.

Gestionar la configuración de la red

Con los ajustes de configuración de red, puede especificar las direcciones LAN y WAN del servidor de gestión para que éste y los servidores de confianza puedan comunicarse.

1. En la ventana de **Añadir/Quitar servicios registrados**, haga clic en **Red**.
2. Especifique la dirección LAN y/o WAN IP del servidor de gestión.

   Si todos los servidores implicados (tanto el servidor de gestión como los servidores de confianza) están en su red local, puede especificar simplemente la dirección LAN. Si uno o varios servidores implicados acceden al sistema a través de una conexión a Internet, debe especificar también la dirección WAN.

3. Haga clic en **Aceptar**.

Propiedades de los servicios registrados

En la ventana de **Añadir servicio registrado** o **Editar servicio registrado**, especifique lo siguiente:

Componente	Requisito
Tipo	Campo ya cumplimentado.
Nombre	Nombre del servicio registrado. El nombre solo se utiliza para mostrarlo en el Management Client.
URL	Haga clic en **Añadir** para añadir la dirección IP o el nombre de host del servicio registrado. Si se especifica un nombre de host como parte de una URL, el host debe existir y estar disponible en la red. Las URL deben comenzar por *http://* o *https://* y no debe contener ninguno de los siguientes caracteres: < > *&* ' " * ? | [ ] ". **Ejemplo** de un formato típico de URL: *http://ipaddress:port/directory* (donde el puerto y el directorio son opcionales). Puede añadir más de una URL si es necesario.
De confianza	Seleccione si el servicio registrado debe ser de confianza inmediatamente (suele ser el caso, pero la opción le da la flexibilidad de añadir el servicio registrado y luego marcarlo como de confianza editando el servicio registrado más tarde).

Componente	Requisito
	Cambiar el estado de confianza también cambia el estado de otros servicios registrados que comparten una o más de las URL definidas para el servicio registrado correspondiente.
Descripción	Descripción del servicio registrado. La descripción solo se utiliza para mostrarla en el Management Client.
Avanzados	Cuando un servicio es avanzado, tiene esquemas URI específicos (por ejemplo, HTTP, HTTPS, TCP o UDP) que deben configurarse para cada dirección de host que se defina. Por lo tanto, una dirección de host tiene múltiples puntos finales, cada uno con su propio esquema, dirección de host y puerto IP para ese esquema.

Eliminación de los drivers de dispositivos (explicación)

Si ya no necesita los controladores de dispositivos en su ordenador, puede eliminar los paquetes de dispositivos de su sistema. Para ello, siga el procedimiento estándar de Windows para eliminar programas.

Si tiene varios paquetes de dispositivos instalados y tiene problemas para eliminar los archivos, puede utilizar el guión de la carpeta de instalación del paquete de dispositivos para eliminarlos por completo.

Si elimina los drivers de los dispositivos, el servidor de grabación y los dispositivos de la cámara ya no podrán comunicarse. No elimine los paquetes de dispositivos cuando actualice, ya que puede instalar una nueva versión sobre una antigua. Solo si desinstala todo el sistema podrá eliminar el paquete de dispositivos.

Eliminar un servidor de grabación

> **!** Si elimina un servidor de grabación, toda la configuración especificada en el Management Client se elimina para el servidor de grabación, incluyendo **todo** el hardware asociado al servidor de grabación (cámaras, dispositivos de entrada, etc.).

1. Haga clic con el botón derecho del ratón en el servidor de grabación que desea eliminar en el panel **Generalidades**.
2. Seleccione **Eliminar servidor de grabación**.
3. Si tiene la certeza, haga clic en **Sí**.
4. El servidor de grabación y todo su hardware asociado son retirados.

Eliminar todo el hardware de un servidor de grabación

> ⚠ Cuando se elimina el hardware, todos los datos registrados relacionados con el hardware se eliminan de forma permanente.

1. Haga clic con el botón derecho del ratón en el servidor de grabación en el que desea eliminar todo el hardware.
2. Seleccione **Borrar todo el hardware**.
3. Confirme la eliminación.

Cambiar el nombre de host del ordenador del servidor de gestión

Si se dirige al servidor de gestión por su nombre de dominio completo (FQDN) o su nombre de host, un cambio en el nombre de host del ordenador tendrá implicaciones en su interior de XProtect que deben ser consideradas y tratadas.

> ⚠ En general, un cambio de nombre de host de un servidor de gestión debe planificarse cuidadosamente debido a la cantidad de limpieza que podría ser necesaria después.

En las siguientes secciones puede obtener una visión general de algunas de las implicaciones de un cambio de nombre de host.

La validez de los certificados

Los certificados se utilizan para cifrar la comunicación entre servicios, y los certificados se instalan en todos los ordenadores que ejecutan uno o varios de los servicios XProtect.

Dependiendo de cómo se creen los certificados, pueden estar relacionados con el ordenador en el que están instalados, y solo serán válidos mientras el nombre del ordenador siga siendo el mismo.

Para obtener más información sobre cómo crear certificados, consulte Introducción a los certificados.

Si se cambia el nombre de un ordenador, los certificados que se utilizan pueden dejar de ser válidos y no se puede iniciar el XProtect VMS. Para que el sistema vuelva a funcionar, siga estos pasos:

- Cree nuevos certificados y reinstálelos en todos los ordenadores del entorno.
- Aplique los nuevos certificados, utilizando el Server Configurator, en cada uno de los ordenadores para habilitar el cifrado con los nuevos certificados.

Esto activará el registro de los nuevos certificados y hará que el sistema vuelva a funcionar.

Pérdida de las propiedades de los datos de los clientes para los servicios registrados

Si completa un registro utilizando el Server Configurator después, por ejemplo, un cambio en la dirección del servidor de gestión, cualquier edición de la información para los servicios registrados se sobrescribirá. Por lo tanto, si ha cambiado la información de los servicios registrados, los cambios deben aplicarse de nuevo para todos los servicios que están registrados en el servidor de gestión en el equipo con el nombre cambiado.

La información que se puede editar para los servicios registrados se ubica en **Herramientas** > **Servicios registrados** > **Editar**:

- De confianza
- Avanzados
- Bandera externa
- Cualquier URL añadida manualmente

En Milestone Customer Dashboard, el nombre del host aparecerá sin cambios

Milestone Customer Dashboard es una herramienta gratuita en línea para Milestonesocios, revendedores y XProtectusuarios de VMS para gestionar y supervisarMilestone instalaciones de software y licencias.

Un cambio de nombre del servidor de gestión en un sistema con el que se ha conectado a Milestone Customer Dashboard no se reflejará automáticamente en Milestone Customer Dashboard.

El antiguo nombre del host aparecerá en Milestone Customer Dashboard hasta que se complete la activación de una nueva licencia. El cambio de nombre, sin embargo, no romperá nada en Milestone Customer Dashboard y una vez que se produce una nueva activación, el registro se actualiza en la base de datos con el nuevo nombre de host. Para obtener más información sobre Milestone Customer Dashboard, consulte Milestone Customer Dashboard (explicación).

Un cambio de nombre de host puede provocar el cambio de la dirección SQL Server

Si se ubica un SQL Server en el mismo ordenador que el servidor de gestión, y se cambia el nombre de este ordenador, la dirección del SQL Server cambiará también. Esto significa que la dirección SQL Server tendrá que ser actualizada para los componentes ubicados en diferentes ordenadores, así como para los componentes en el ordenador local que utilizan el nombre del ordenador en lugar de localhost para conectarse al SQL Server. Esto se aplica específicamente al Event Server que utiliza la misma base de datos que el Management Server. También podría aplicarse al Log Server que utiliza una base de datos diferente pero muy probablemente en el mismo servidor SQL.

Para más información sobre cómo actualizar las direcciones SQL del Event Server y del Management Server, consulte Cambiar las direcciones SQL del servidor de gestión y del servidor de eventos. La dirección del servidor SQL para el Log Server debe ser actualizada en el Registro de Windows.

Cambios de nombre de host en un Milestone Federated Architecture

Los cambios en el nombre de un ordenador que esté dentro de una configuración Milestone Federated Architecture tendrán las siguientes implicaciones, y esto se aplica tanto cuando los sitios están conectados dentro de los grupos de trabajo como a través de los dominios.

El host del sitio es el nodo raíz de la arquitectura

Si cambia el nombre del ordenador en el que se ejecuta el sitio central dentro de la arquitectura, todos los nodos secundarios se volverán a conectar automáticamente a la nueva dirección. Así que en este caso, un cambio de nombre no requerirá ninguna acción.

El host del sitio es un nodo hijo en la arquitectura

Para evitar problemas de conexión al cambiar el nombre de un ordenador en el que se ejecutan uno o varios sitios federados, debe añadir una dirección alternativa al sitio afectado, antes de cambiar el nombre del ordenador. El sitio afectado es el nodo cuyo ordenador central será renombrado. Para obtener más información sobre los problemas de conexión debidos a cambios de nombre de host no preparados o imprevistos y cómo resolver los problemas, consulte Problema: Un nodo principal en una configuración de Milestone Federated Architecture no puede conectar con un nodo secundario.

La dirección alternativa debe añadirse en el panel de **Propiedades**, ya sea en el panel de **Navegación del sitio** o en el de **Jerarquía del sitio federado**. Deben cumplirse los siguientes requisitos previos:

- La dirección alternativa debe añadirse para que esté disponible antes de que se cambie el nombre del ordenador central
- La dirección alternativa debe reflejar el futuro nombre del ordenador central (cuando se cambie de nombre)

Consulte Establecer propiedades del sitio para obtener información sobre cómo acceder al panel **Propiedades**.

> Para garantizar una actualización lo más fluida posible, detenga el Management Client en el nodo que sirve como nodo principal al que cambiará su nombre de host. De lo contrario, detenga y reinicie el cliente después de que el ordenador haya sido renombrado. Para obtener más información, consulte Iniciar o detener el servicio Management Server.

> Además, asegúrese de que la dirección alternativa que proporcionó se refleja en el panel de **Jerarquía de sitios federados** en su sitio central y, si no es así, detenga y reinicie el Management Client.

Una vez que se haya renombrado el host y se haya reiniciado el ordenador, el sitio federado cambiará automáticamente a la nueva dirección.

Registros del servidor de gestión

Lo siguiente son los tipos de registros del servidor:

- Registro del sistema
- Registro de auditoría
- Registros activados por reglas

Estos se usan para registrar el uso del sistema. Estos registros están disponibles en el Management Client en **Registros del servidor**.

Para obtener información sobre registros utilizados para la resolución de problemas e investigar errores de software, consulte Registros de depuración (explicación) en la página 381.

Identificar actividad del usuario, eventos, acciones y errores

Utilice registros para obtener un registro detallado e la actividad el usuario, eventos, acciones y errores en el sistema.

Para ver registros en Management Client, vaya al panel **Navegación por el sitio** y seleccione **Registros del servidor**.

Tipo de registro	¿Qué se ha registrado?
Registros del sistema	Información relacionada con el sistema
Registros de auditoría	Actividad del usuario
Registros activados por reglas	Reglas en las que los usuarios han especificado la acción **Crear nueva <entrada de registro>**. Para obtener información adicional sobre la acción <entrada de registro>, consulte Accione y acciones de parada.

Para ver registros en un idioma distinto, consulte Pestaña General (opciones) en la página 397 en **Opciones**.

Para exportar registros como archivos de valores separados por comas (.csv), consulte Exportar registros.

Para cambiar los ajustes de registro, consulte Pestaña Registros del servidor (opciones) en la página 400.

Filtrar registros

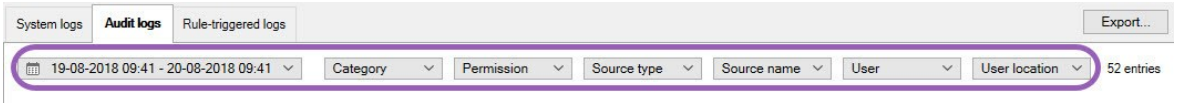
En cada ventana de registro, puede aplicar filtros para ver entradas de registro, por ejemplo, de un lapso de tiempo, un dispositivo o un usuario concretos.

> Los filtros se generan de las entradas de registros que están actualmente visibles en la interfaz de usuario.

1. En el panel **Navegación por el sitio**, seleccione **Registros del servidor**. De forma predeterminada, aparece la pestaña **Registros del sistema**.

   Para navegar entre tipos de registro, seleccione una pestaña distinta.

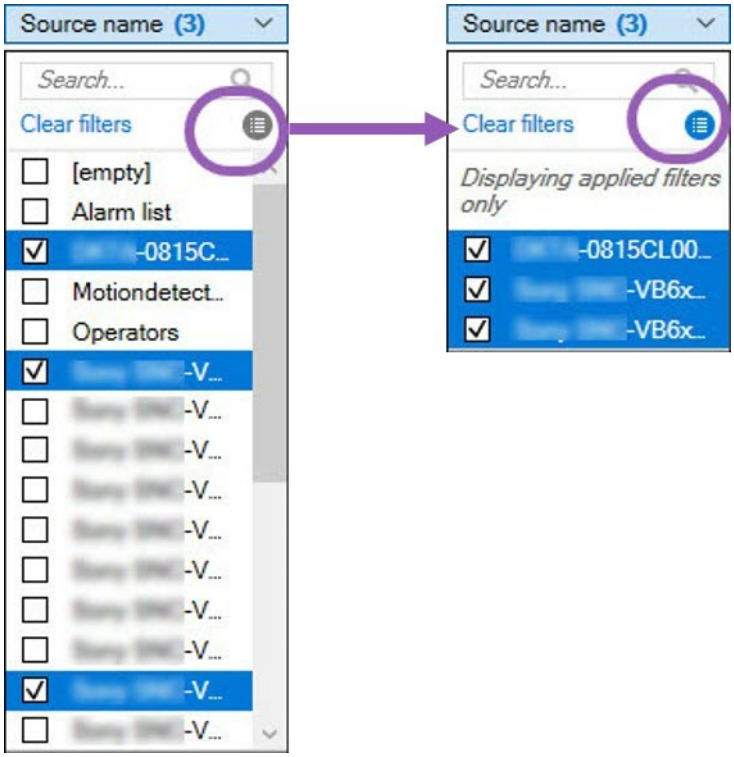
2. En las pestañas, seleccione un grupo de filtros, por ejemplo, **Categoría**, **Tipo de fuente** o **Usuario**.



   Aparece una lista de filtros. Una lista de filtros muestra un máximo de 1000 filtros.

3. Seleccione un filtro al que aplicarlo. Seleccione un filtro de nuevo para quitarlo.

   Opcional: En una lista de filtros, seleccione, seleccione **Mostrar solo filtros aplicados** para ver solo los filtros que aplicó.



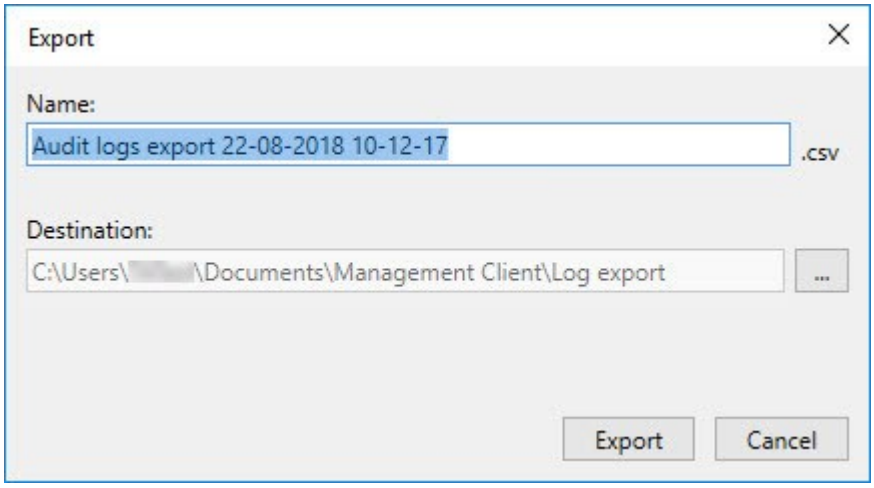
> Al exportar registros, el contenido de su exportación cambia dependiendo de los filtros que aplique. Para obtener información sobre su exportación, consulte Exportar registros.

Exportar registros

Exportar registros le ayuda, por ejemplo, a guardar entradas de registro más allá del periodo de retención de registros. Puede exportar registros como archivos de valores separados por comas (.csv).

Para exportar un registro:

1. Seleccione **Exportar** en la esquina superior derecha. Aparece la ventana **Exportar**.



2. En la ventana **Exportar**, en el campo **Nombre**, especifique un nombre en el archivo de registro.
3. De forma predeterminada, los archivos de registro exportados se guardan en su carpeta **Exportación de registros**. Para especificar una ubicación diferente, seleccione ... a la derecha del campo **Destino**.
4. Seleccione **Exportar** para exportar el registro.

> El contenido de la exportación cambia dependiendo de los filtros que aplique. Para obtener información sobre su exportación, consulte Filtrar registros.

Registros de búsqueda

Para buscar un registro, utilice **Criterios de búsqueda** en la parte superior del panel de registros:

1. Especifique sus criterios de búsqueda de la listas.
2. Haga clic en **Actualizar** para que la página de registros refleje sus criterios de búsqueda. Para borrar sus criterios de búsqueda y volver a a ver todo el contenido del registro, haga clic en **Borrar**.

Puede hacer doble clic en cualquier fila para que se presenten todos los detalles en una ventana **Detalles del registro**. De este modo, también puede leer entradas de registros que contienen más texto del que se puede mostrar en una sola línea.

Cambiar idioma del registro

1. En la parte inferior del panel de registros, en la lista **Mostrar inicio de sesión**, seleccione el idioma deseado.

2. El registro se muestra en el idioma seleccionado. La próxima vez que abra el registro, se restablecer al idioma predeterminado.

Permita que 2018 R2 y los componentes anteriores escriban registros

La versión 2018 R3 del servidor de registros introduce la autenticación para una seguridad añadida. Esto evita que componentes 2018 R2 y anteriores escriban registros en el servidor de registros.

Componentes afectados:

- XProtect Smart Client
- Plug-in XProtect LPR
- LPR Server
- Plug-in de control de acceso
- Event Server
- Plug-in de alarma

Si está utilizando la versión 2018 R2 o una versión previa de cualquiera de los componentes enumerados previamente, debe decidir si permite o no que el componente escriba registros en el nuevo servidor de registros:

1. Seleccione **Herramientas** > **Opciones**.
2. En el cuadro de diálogo **Opciones**, en la parte inferior de la pestaña **Registros de servidores**, encuentre la casilla de verificación **Permitir 2018 R2 y componentes anteriores para escribir registros**.
    - Seleccionar la casilla de verificación para permitir que componentes 2018 R2 y anteriores escriban registros
    - Desactivar la casilla de verificación para no permitir que 2018 R2 y componentes anteriores escriban registros

Solución de problemas

Registros de depuración (explicación)

Los registros de depuración se usan para identificar defectos y fallos de seguridad en el sistema.

Para obtener información sobre regustros utilizados para el uso del sistema, consulte Registros del servidor de gestión en la página 376.

Lo siguiente son las ubicaciones de los archivos de registro en la instalación de XProtect:

- `C:\ProgramData\Milestone\IDP\Registros`

  > Esto es accesible solo para usuarios de IIS y administradores. Si el usuario de IIS cambia, estos permisos deben actualizarse.

- `C:\ProgramData\Milestone\MIPSDK`
- `C:\ProgramData\Milestone\XProtect Data Collector Server\Registros`
- `C:\ProgramData\Milestone\XProtect Servidor de evento\Registros`
- `C:\ProgramData\Milestone\XProtect Servidor de registro`
- `C:\ProgramData\Milestone\XProtect Servidor de gestión\Registros`
- `C:\ProgramData\Milestone\XProtect Mobile Servidor\Registros`
- `C:\ProgramData\Milestone\XProtect Servidor de grabación\Registros`
- `C:\ProgramData\Milestone\XProtect Servidor web de informes\Registros`

Emitir: El cambio de direcciones de bases de datos y SQL Server previene el acceso a las bases de datos

Si las direcciones al SQL Server y la base de datos se cambian, por ejemplo, cambiando el nombre del hostdel ordenador que ejecuta el SQL Server,el accso del servidor de grabaciones a la base de datos se pierde.

Solución: Cambie el nombre del SQL Server y las direcciones de bases de datos a través del Registro de Windows.

Para obtener más información sobre el cambio de las direcciones de los SQL Server y de las bases de datos, consulte Gestión del servidor SQL y de las bases de datos .

Emitir: El inicio del servidor de grabaciones falla debido a un conflicto de puertos

Este problema solo puede aparecer si el protocolo para transferencia simple de correo (SMTP) se está ejecutando, ya que utiliza el puerto 25. Si el puerto 25 ya está en uso, puede que no sea posible iniciar el servicio Recording Server. Es importante que el número de puerto 25 esté disponible para el servicio SMTP del servidor de grabaciones.

Servicio SMTP: Verificación y soluciones

Para verificar si el Servicio SMTP está instalado:

1. En el menú **Inicio** de Windows, seleccione **Panel de control**.
2. En el **Panel de control**, haga doble clic en **Agregar o quitar programas**.
3. En el lado izquierdo de la ventana **Añadir o quitar programas**, haga clic en **Añadir/Quitar componentes de Windows**.
4. En el asistente **Componentes de Windows**, seleccione **Servicios de información de Internet (IIS)** y haga clic en **Detalles**.
5. En la ventana **Servicio de información de Internet (IIS)**, verifique si la casilla de verificación **Servicio SMTP** está seleccionada. Si es así, el Servicio SMTP está instalado.

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

Solución 1: Deshabilitar Servicio SMTP o establecerlo en inicio manual

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

1. En 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 **Herramientas administrativas**, haga doble clic en **Servicios**.
4. En la ventana **Servicios**, haga doble clic en **Protocolo de transferencia de correo simple (SMTP)**.
5. En la ventana **Propiedades de SMTP**, haga clic en **Detener**, luego establezca **Tipo de inicio** en **Manual** o **Deshabilitado**.

   Cuando se establece en **Manual**, el servicio SMTP se puede iniciar manualmente desde la ventana **Servicios**, o desde una ventana de comandos utilizando el comando *net start SMTPSVC*.
6. Haga clic en **Aceptar**.

Solución 2: Servicio SMTP

Quitar el servicio SMTP puede afectar a otras aplicaciones que utilizan el servicio SMTP.

1. En el menú **Inicio** de Windows, seleccione **Panel de control**.
2. En la ventana **Panel de control**, haga doble clic en **Agregar o quitar programas**.
3. En el lado izquierdo de la ventana **Añadir o quitar programas**, haga clic en **Añadir/Quitar componentes de Windows**.
4. En el asistente **Componentes de Windows**, seleccione el elemento **Servicios de información de Internet (IIS)** y haga clic en **Detalles**.
5. En la ventana **Servicios de información de Internet (IIS)**, desactive la casilla de verificación de **Servicio SMTP**.
6. Haga clic en **Aceptar**, **Siguiente** y **Terminar**.

Emitir: Recording Server pasa a estar fuera de línea al cambiar al nodo del clúster de Management Server

Si configura un clúster de Microsoft para Management Server redundancia, Recording Server o Recording Server pueden desconectarse al cambiar Management Server entre nodos de clústeres.

Para corregir esto, haga lo siguiente:

> Al realizar cambios en la configuración en el Gestor de clústeres de failover de Microsoft, pause el control y monitorice el servicio para que Server Configurator pueda hacer cambios e iniciar y/o parar el servicio de Management Server. Si cambia el tipo de inicio del servicio de clúster de failover, no debe provocar ningún conflicto con el Server Configurator.

En los ordenadores de Management Server:

1. Inicie Server Configurator en cada uno de los ordenadores que tienen un servidor de gestión instalado.
2. Vaya a la página **Registro**.
3. Haga clic en el símbolo del lápiz ( ) para que la dirección del servidor de gestión sea editable.
4. Cambie la dirección del servidor de gestión a la URL del clúster, por ejemplo **http://MyCluster**.
5. Haga clic en **Registrar**.

En ordenadores que tienen componentes que utilizan el Management Server (por ejemplo, Recording Server, Mobile Server, Event Server, API Gateway):

1. Inicie Server Configurator en cada uno de los ordenadores.
2. Vaya a la página **Registro**.
3. Cambie la dirección del servidor de gestión a la URL del clúster, por ejemplo **http://MyCluster**.
4. Haga clic en **Registrar**.

Emitir: Un nodo principal en una configuración de Milestone Federated Architecture no puede conectar con un nodo secundario

Si ha cambiado el nombre del ordenador host de un sitio que actúa como un nodo secundario en un Milestone Federated Architecture, un nodo principal no podrá conectarse a él

Para restablecer la conexión entre el nodo principal y el sitio

- Desasociar el sitio afectado de su principal. Para obtener información adicional, consulte Quitar un sitio de la jerarquía.
- Vuelva a conectar el sitio utilizando el nombre nuevo o su host. Para obtener información adicional, consulte Añadir sitio a jerarquía.

> Para asegurarse de que los cambios tienen efecto, podría querer detener y reiniciar Management Client en el nodo que sirve como nodo principal para aquel cuyo nombre de host ha cambiado. Para obtener más información, consulte Iniciar o detener el servicio Management Server.

Para obtener información adicional sobre las implicaciones de un cambio de nombre de host en una configuración de Milestone Federated Architecture, consulte Cambios de nombre de host en un Milestone Federated Architecture.

Actualizar

Actualizar (explicación)

Al actualizar, todos los componentes actualmente instalados en el ordenador se actualizan. No es posible eliminar componentes instalados durante una actualización. Si quiere quitar componentes instalados, utilice la funcionalidad **Añadir y quitar programas** de Windows antes o después de una actualización. Durante la actualización, todos los componentes, excepto la base de datos del servidor de gestión, se eliminan automáticamente y se reemplazan. Esto incluye los controladores de su paquete de dispositivos.

La base de datos del servidor de gestión contiene la configuración entera del sistema (configuraciones del servidor de grabación, configuraciones de cámaras, reglas, etc.). Siempre que no quite la base de datos del servidor de gestión, no es necesario reconfigurar la configuración de su sistema, incluso si puede querer configurar algunas de las funciones nuevas en la versión nueva.

La retrocompatibilidad con servidores de grabación de versiones de XProtect anteriores a la versión actual es limitada. Aún puede acceder a grabaciones en dichos servidores de grabación más antiguos, pero para cambiar su configuración, deben ser de la misma versión que este. Milestone recomienda que actualice todos los servidores de grabación de su sistema.

Al actualizar incluidos sus servidores de grabación, se le pregunta si quiere actualizar o mantener los controladores de los dispositivos de vídeo. Si opta por actualizar, podría tardar unos minutos que sus dispositivos de hardware conectaran con los controladores de dispositivos de vídeo nuevos después de reiniciar su sistema. Esto se debe a varias comprobaciones internas en los controladores recién instalados.

Si actualizada desde la versión 2017 R3 o anterior a la versión 2018 R1 o posterior, y si su sistema tiene cámaras más antiguas, debe descargar manualmente el paquete de dispositivos con controladores existentes de la página de descargas en nuestro sitio web (https://www.milestonesys.com/downloads/). Para ver si tiene cámaras que utilizan controladores en el paquete de dispositivos existente, visite esta página en nuestro sitio web (https://www.milestonesys.com/community/business-partner-tools/device-packs/).

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 sus sistema con un parche de seguridad antes de actualizar. Actualizar sin el parche de seguridad, provocará que los servidores de grabación fallen.

Las instrucciones para instalar el parche de seguridad en sus servidores de grabación están disponibles en nuestro sitio webhttps://supportcommunity.milestonesys.com/s/article/XProtect-VMS-NET-security-vulnerability-hotfixes-for-2016-R1-2018-R1/.

Si quiere encriptar la conexión entre el servidor de gestión y los servidores de grabación, todos los servidores de grabación deben actualizarse a 2019 R2 o más reciente.

Requisitos de actualización

- Tenga preparado el archivo de licencia del software (consulte Licencias (explicación) en la página 117) (.lic):
  - **Actualización del paquete de servicio**: Durante la instalación del servidor de gestión, el asistente le pide que especifique la ubicación del archivo de licencia de software. Puede utilizar tanto el archivo de licencia de software que recibió tras comprar su sistema (o la actualización más reciente) y el archivo de licencia de software activado que obtuvo después de la actualización de su última licencia
  - **Actualización de la versión**: Después de haber comprado la nueva versión, recibe un nuevo archivo de licencia de software. Durante la instalación de un servidor de gestión, el asistente le pide que especifique la buicación del archivo de licencia de software nuevo

  El sistema verifica el archivo de licencia de software antes de que pueda continuar. Los dispositivos de hardware ya añadidos y otros dispositivos que requieren licencias entrarán en un periodo de gracia. Si no ha habilitado la activación de licencia automática (consulte Activar la activación automática de licencia en la página 124), recuerde activar sus licencias manualmente antes de que venza el periodo de gracia. Si no tiene su archivo de licencia de software, póngase en contacto con su revendedor de XProtect.
- Tenga preparado el software de la **nueva versión del producto**. Puede descargarlo desde la página de descarga en el sitio web de Milestone.

- Asegúrese de que ha hecho una copia de seguridad de la configuración del sistema (consulte Hacer una copia de seguridad y restaurar la configuración del sistema (explicación) en la página 340)

  El servidor de gestión almacena la configuración del sistema en una base de datos SQL. La base de datos SQL puede estar ubicada en un SQL Server en la propia máquina del servidor de gestión en un SQL Server en la red.

  Si utiliza una base de datos SQL en una SQL Server en su red, el servidor de gestión debe tener permisos de administrador en el SQL Server siempre que quiera crear, mover o actualizar la base de datos SQL. Para el uso y el mantenimiento regulares de la base de datos SQL, el servidor de gestión solo necesita ser propietario de la base de datos SQL.

- Si tiene pensado habilitar la encriptación durante la instalación, necesita tener los certificados apropiados instalados y deben ser confiables en los ordenadores relevantes. Si desea más información, consulte Comunicación segura (explicación) en la página 150.

Cuando esté listo para empezar a actualizar, siga los procedimientos en Actualizar prácticas recomendadas en la página 389.

Actualizar XProtect VMS para ejecutar en modo compatible con FIPS 140-2

Desde la versión 2020 R3, XProtect VMS está configurado para ejecutarse de modo que utilice solo las instancias de algoritmos certificados por FIPS 140-2.

Para obtener información detallada sobre cómo configurar su XProtect VMS para que se ejecute en modo compatible con FIPS 140-2, consulte la sección de cumplimiento de FIPS 140-2 la guía de endurecimiento.

> **!** En el caso de los sistemas que cumplan con FIPS 140-2, con exportaciones y bases de datos de medios archivados de versiones de XProtect VMS anteriores a 2017 R1 que estén cifrados con cifrados que no cumplan con FIPS, es necesario archivar los datos en una ubicación en la que se pueda seguir accediendo a ellos después de habilitar FIPS.

El siguiente proceso describe qué es necesario para configurar XProtect VMS para ejecutar en modo compatible con FIPS 140-2:

1. Deshabilite la política de seguridad FIPS de Windows en todos los ordenadores que forman parte del VMS, incluido el ordenador que aloja el servidor SQL.

   Al actualizar, no puede instalar XProtect VMS cuando FIPS se habilita en el sistema operativo Windows.

2. Garantiza que las integraciones independientes de terceros puedan ejecutarse en un sistema operativo Windows habilitado para FIPS.

   Si una integración individual no es compatible con FIPS 140-2, no se puede ejecutar después de establecer el sistema operativo set Windows para operar en modo FIPS.

   Para evitar eso:

   - Hacer un inventario de todas las integraciones independientes en XProtect VMS
   - Contacte con los proveedores de estas integraciones pregúnteles si las integraciones se ajustan a FIPS 140-2
   - Desplegar las integraciones independientes compatibles con FIPS 140-2

3. Garantice que los controladores y, por tanto, la comunicación con los dispositivos, cumple FIPS 140-2.

   XProtect VMS está garantizado y puede forzar el modo de funcionamiento compatible con FIPS 140-2 si se cumplen los siguientes criterios:

   - Los dispositivos solo usan controladores compatibles para conectar se a XProtect VMS

     Consulte la sección de cumplimiento de FIPS 140-2 en la guía para reforzar para obtener más información sobre drivers que pueden asegurar y hacer cumplir la normativa.

   - Los dispositivos utilizan la versión 11.1 o superior del paquete de dispositivos

     Los controladores de los paquetes de dispositivos de controladores existentes no pueden garantizar una conexión compatible con FIPS 140-2.

   - Los dispositivos están conectados a través de HTTPS y en el Protocolo de transporte seguro en tiempo real (Secure Real-Time Transport Protocol, SRTP) o el Protocolo de transmisión en tiempo real (Real Time Streaming Protocol, RTSP) a través de HTTPS para el flujo de video.

     Los módulos de controlador no garantizar el cumplimiento con FIPS 140-2 de una conexión por HTTP. La conexión puede ser compatible, pero no existen garantías de que sea efectivamente compatible.

   - El ordenador que está ejecutando el servidor de grabación ejecuta el SO Windows con el modo FIPS habilitado

4. Garantice que los datos de la base de datos de medios esté encriptada con cifrados compatibles con FIPS 140-2.

   Esto se hace ejecutando la herramienta de actualización de la base de datos de medios. Para obtener información detallada sobre cómo configurar su XProtect VMS para que se ejecute en modo compatible con FIPS 140-2, consulte la sección de cumplimiento de FIPS 140-2 la guía de endurecimiento.

5. Antes de habilitar FIPS en el sistema operativo de Windows, y después de que haya configurado su sistema XProtect VMS y de que se haya asegurado de que todos los componentes y dispositivos pueden ejecutarse en un entorno habilitado para FIPS, actualice las contraseñas del hardware existente en XProtect Management Client.

   Para hacerlo, en el Management Client, desde el servidor de grabación seleccionado en el nodo **Servidores de grabación**, haga clic con el botón derecho y seleccione **Añadir hardware**. Avance por el asistente **Añadir hardware**. Esto actualizará todas las credenciales actuales y las encriptará para ser compatibles con FIPS.

Puede habilitar FIPS solo después de haber actualizado todo el VMS, incluidos todos los clientes.

Actualizar prácticas recomendadas

Lea sobre los requisitos de actualización (consulte Requisitos de actualización en la página 386) incluida la copia de seguridad de la base de datos antes de iniciar la actualización real.

> Los controladores de dispositivos ahora se dividen en dos paquetes de dispositivos: el paquete de dispositivos normal con controladores más nuevos y el paquete de dispositivos existentes con controladores antiguos. El paquete de dispositivos regular siempre se instala automáticamente con una actualización o mejora. Si tiene cámaras más antiguas que utilizan controladores de dispositivos del paquete de dispositivos existentes y aún no tiene ya un paquete de dispositivos existentes, el sistema no instala automáticamente el paquete de dispositivos existente.

> Si su sistema tiene cámaras más antiguas, Milestone recomienda que compruebe si la cámara utiliza controladores del paquete de dispositivos existentes en esta página (https://www.milestonesys.com/community/business-partner-tools/device-packs/). Para comprobar si tiene el paquete existente ya instalado, mire en carpetas del sistema de XProtect. Si necesita descargar el paquete de dispositivos existente, vaya a la página de descarga (https://www.milestonesys.com/downloads/).

Si su sistema es un sistema de **un único ordenador**, puede instalar el nuevo software sobre la instalación existente.

En un sistema Milestone Interconnect o Milestone Federated Architecture, debe iniciar la actualización del sitio central y posteriormente de los sitios remotos.

En un sistema distribuido, realice la actualización en este orden:

1. Actualice el servidor de gestión con la opción **Personalizar** en el instalador (consulte Instale su sistema: opción personalizada en la página 163).
    1. En la página del asistente en la que elija componentes, todos los componentes del servidor de gestión están preseleccionados.
    2. Especifique el SQL Server y la base de datos. Decida si conservar la base de datos SQL que ya está utilizando para conservar los datos existentes en la base de datos.

    > Al iniciar la instalación, se pierde la funcionalidad del servidor de grabación de failover (consulte Servidor de grabación de failover (explicación) en la página 37).

    > Si habilita la encriptación en el servidor de gestión, los servidores de grabación están fuera de línea hasta que habilite la encriptación en el servidor de gestión (consulte Comunicación segura (explicación) en la página 150).

2. Actualizar servidores de grabación de failover. Desde la página web de descarga del servidor de gestión (controlada por Download Manager), instale Recording Server.

    > Si tiene pensado habilitar la encriptación para los servidores de grabación de failover y quiere conservar la funcionalidad de failover, actualice el servidor de grabación de failover sin encriptación y habilítelo si ha actualizado los servidores de grabación.

    En este punto, la funcionalidad del servidor de failover vuelve a funcionar.

3. Si tiene pensado habilitar la encriptación desde servidores de gestión o servidores de gestión de failover en los clientes y es importante que los clientes puedan recuperar datos durante la actualización, actualice todos los clientes y servicios que recuperen flujos de datos de los servidores de grabación antes de actualizar los servidores de grabación. Estos clientes y servicios son:
    - XProtect Smart Client
    - Management Client
    - Management Server
    - Servidor XProtect Mobile
    - XProtect Event Server
    - DLNA Server Manager

- Milestone Open Network Bridge
- Sitios que recuperan flujos de datos del servidor de grabación mediante Milestone Interconnect
- Algunas integraciones de MIP SDK de terceros

4. Actualice los servidores de grabación. Puede instalar servidores de grabación utilizando el asistente de instalación (consulte Instalar un servidor de grabación a través de Download Manager en la página 171) o de manera silenciosa (consulte Instalar un servidor de grabación de forma silenciosa en la página 179). La ventaja de una instalación silenciosa es que puede hacerla de manera remota.

> **!** Si habilita la encriptación y el certificado de autenticación del servidor seleccionado no es de confianza en todos los ordenadores relevantes en ejecución, pierden la conexión. Si desea más información, consulte Comunicación segura (explicación) en la página 150.

Continúe con estos pasos para los demás sitios de su sistema.

Actualizar en un clúster

Asegúrese de que tiene una copia de seguridad de la base de datos antes de actualizar el clúster.

1. Detenga el servicio de Management Server en todos los servidores de gestión del clúster.
2. Desinstale el servidor de gestión en todos los servidores del clúster.
3. Utilice el procedimiento para instalar varios servidores de gestión en un clúster, tal como se describe para instalar en un clúster. Consulte Instalar en un clúster en la página 183.

> **!** Al instalar, asegúrese de reutilizar el SQL Server existente y la base de datos SQL existente que actualmente almacena la configuración del sistema. La configuración del sistema se actualiza automáticamente.

Detalles de interfaz de usuario

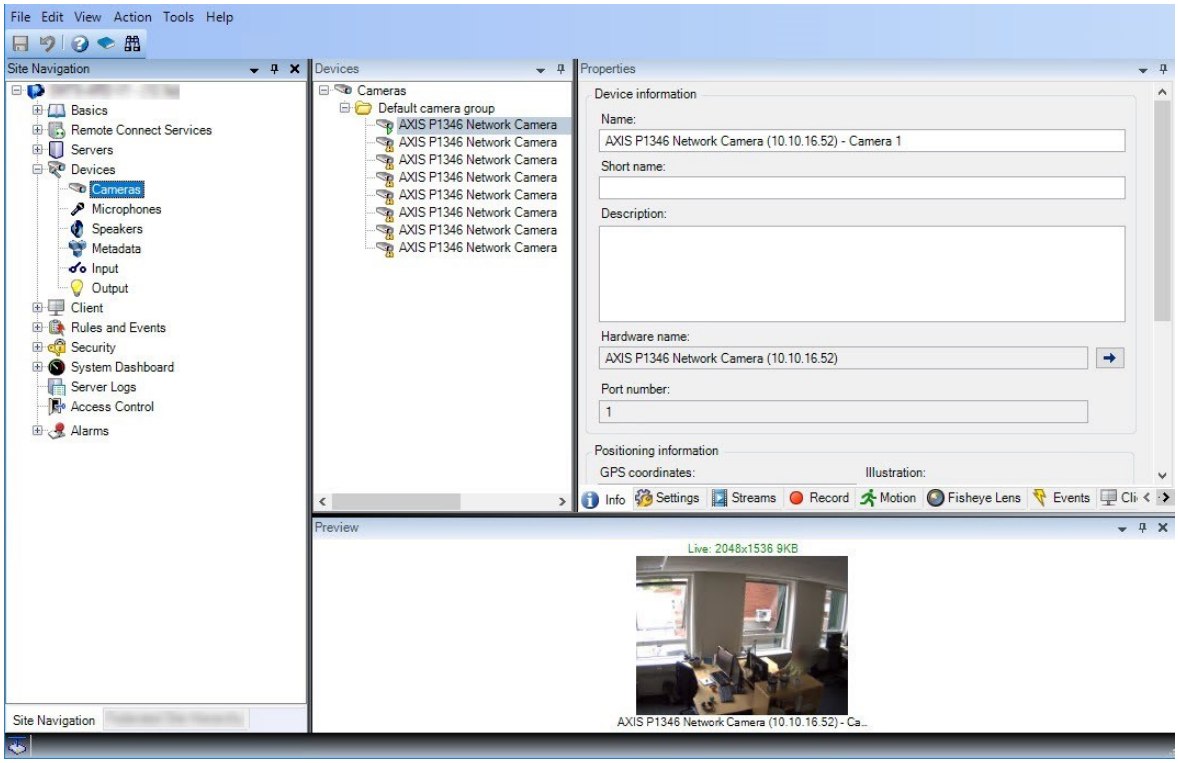
Ventana y paneles principales

La ventana de Management Client se divide en paneles. El número de paneles y diseño depende de usted:

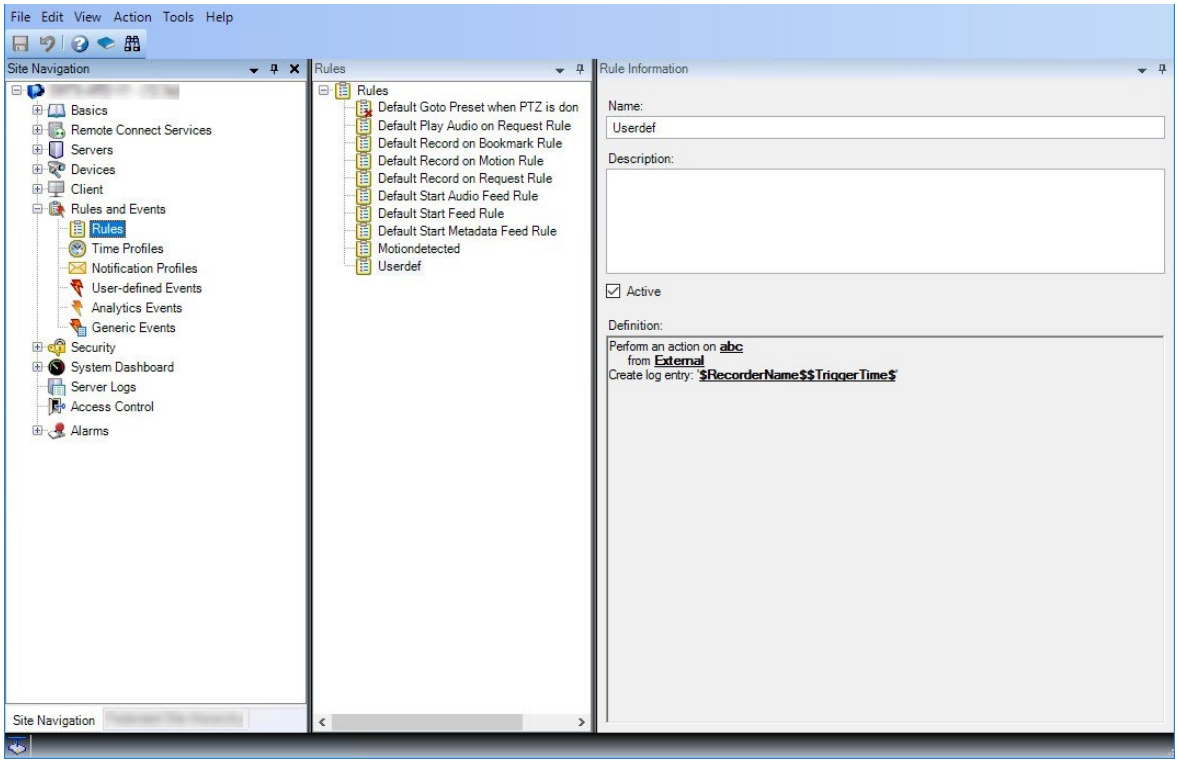
- Configuración del sistema
- Tarea
- Funciones disponibles

A continuación se muestran algunos ejemplos de diseños típicos:

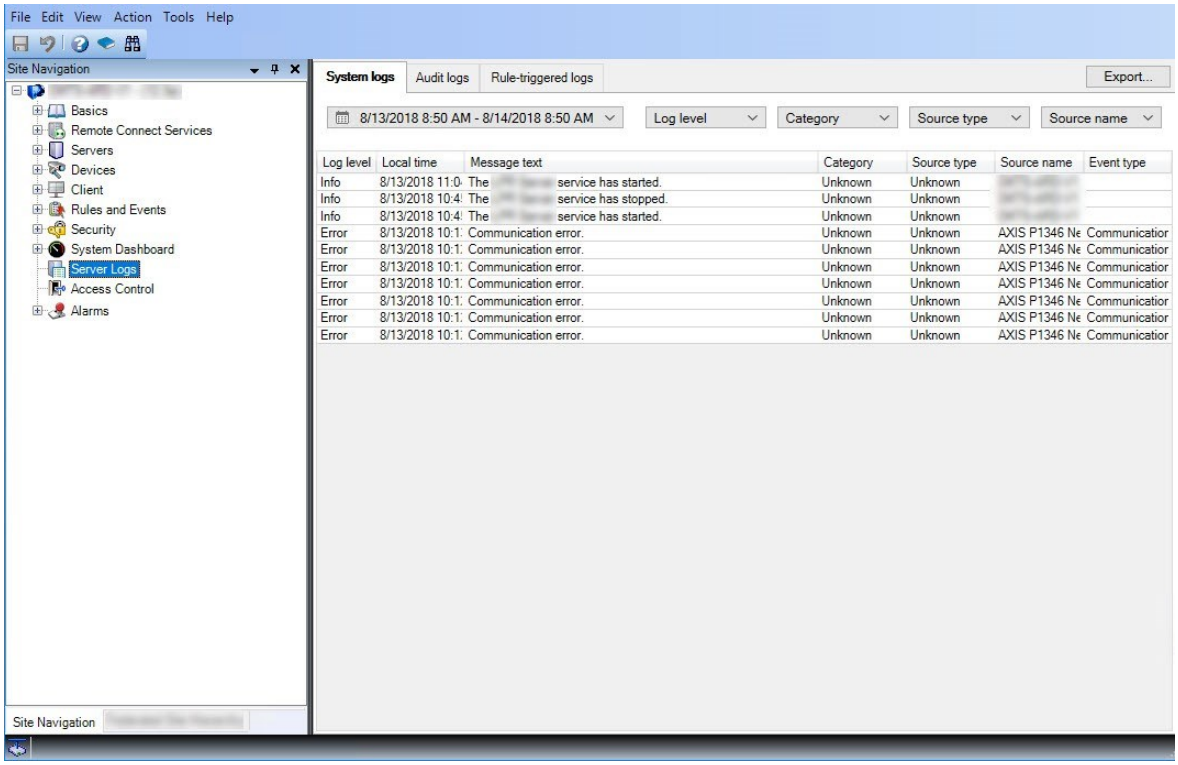
- Cuando trabaja con servidores y dispositivos de grabación:



- Cuando trabaja con reglas, perfiles de tiempo y notificación, usuarios, roles:

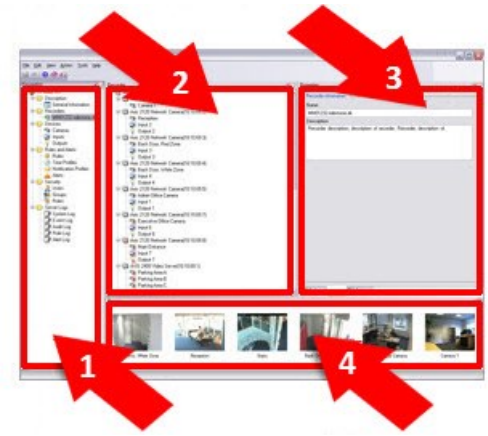


- Cuando ve registros:



Diseño de paneles

La ilustración describe un diseño de ventana típico. Puede personalizar el diseño de modo que puede aparecer de manera distinta en su ordenador.



1. Pan el Navegación por el sitio y panel Jerarquía de sitios federados
2. Panel de generalidades
3. Panel de propiedades
4. Panel Vista previa

Panel Navegación por el sitio

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

En el panel **Navegación por el sitio**, puede configurar y gestionar su sistema para que coincida con sus necesidades. Si su sistema no es un sistema de un único sitio, pero incluye sitios federados, tenga en cuenta que gestiona estos sitios en el panel **Jerarquía de sitios federados**.

La funcionalidad disponible depende del sistema que esté utilizando. Vea la lista completa de características, que está disponible en la página de descripción del producto en el sitio web Milestone (https://www.milestonesys.com/solutions/platform/product-index/).

Panel Jerarquía de sitios federados

Este en su elemento de navegación que muestra todos los sitios de Milestone Federated Architecture en una jerarquía de sitios principal/secundario.

Puede seleccionar cualquier sitio, iniciar sesión en él y se inicia el Management Client para ese sitio. El sitio en el que ha iniciado sesión siempre aparecer en la parte superior de la jerarquía.

Panel de generalidades

Proporciona una descripción general del elemento que ha seleccionado en el panel **Navegación por el sitio**, por ejemplo, como una lista detallada. Cuando seleccione un elemento en el panel **Descripción general**, normalmente muestra las propiedades en el panel **Propiedades**. Al hacer clic con el botón derecho en el panel **Descripción general** obtiene acceso a las características de gestión.

Panel de propiedades

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

Panel Vista previa

El panel **Vista previa** aparece al trabajar con dispositivos y servidores de grabación. Muestra imágenes de vista previa desde las cámaras seleccionadas o muestra información sobre el estado del dispositivo. El ejemplo muestra una imagen de vista previa de la cámara con información sobre la resolución y la velocidad de datos del flujo en directo de la cámara:

De forma predeterminada, la información que se muestra con las imágenes de vista previa de la cámara se refiere a flujos en directo. Esto se muestra en texto verde encima de la vista previa. Si, en su lugar, quiere información sobre el flujo de grabación texto rojo), seleccione **Ver** > **Mostrar flujos de grabación** en el menú.

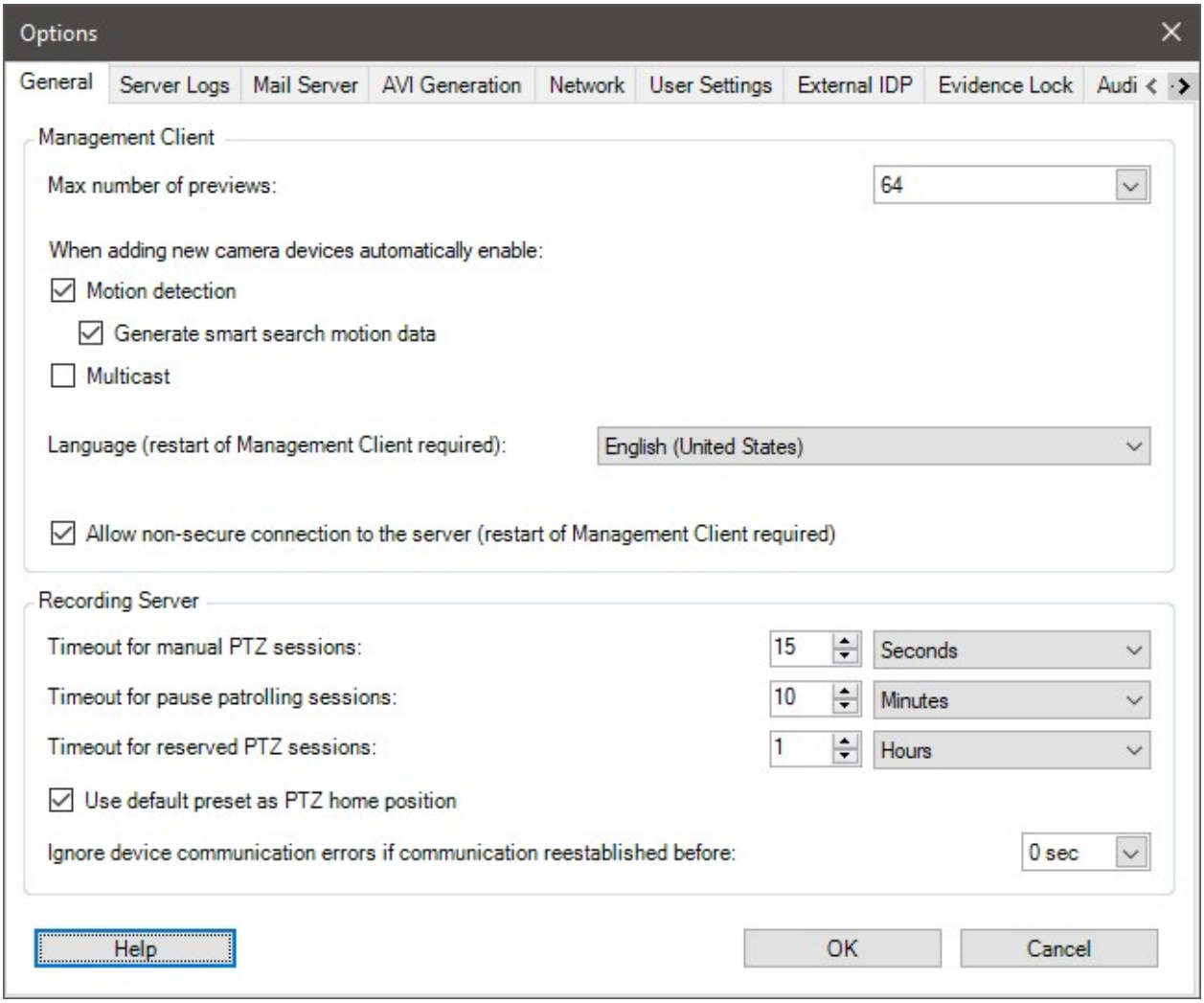
El rendimiento puede verse afectado si el panel **Vista previa** muestra imágenes de vista previa desde muchas cámaras a una alta velocidad de fotogramas. Para controlar el número de imágenes de vista previa y su velocidad de fotogramas, seleccione **Opciones** > **General** en el menú.

Ajustes del sistema (cuadro de diálogo Opciones)

En el cuadro de diálogo **Opciones**, puede especificar una serie de ajustes relacionados con el aspecto general y la funcionalidad del sistema.

La funcionalidad disponible depende del sistema que esté utilizando. Vea la lista completa de características, que está disponible en la página de descripción del producto en el sitio web Milestone (https://www.milestonesys.com/solutions/platform/product-index/).

Para acceder al cuadro de diálogo, seleccione **Herramientas** > **Opciones**.



Pestaña General (opciones)

En la pestaña General, puede especificar ajustes generales para el Management Client y el servidor de grabación.

Management Client

Nombre	Descripción
Número máximo de vistas previas	Seleccione el número máximo de imágenes en miniatura mostradas en el panel **Vista previa**. El valor predeterminado

Nombre	Descripción
	es 64 imágenes en miniatura. Seleccione **Acción** > **Actualizar** desde el menú para que el cambio tenga efecto. Un gran número de imágenes en miniatura en combinación con una elevada velocidad de fotogramas puede ralentizar el sistema.
Al añadir dispositivos de cámaras nuevos, automáticamente se habilita: **Detección de movimiento**	Seleccione la casilla de verificación para habilitar la detección de movimiento en las cámaras nuevas cuando las añada al sistema con el asistente **Añadir hardware**. Este ajuste no afecta a los ajustes de detección de movimiento en las cámaras existentes. La detección de movimiento para una cámara se habilita y deshabilita en la pestaña **Movimiento** para el dispositivo de cámara.
Al añadir dispositivos de cámaras nuevos, automáticamente se habilita: **Generar datos de movimiento para búsqueda inteligente**	La generación de datos de movimiento para la búsqueda inteligente requiere que la detección de movimiento esté habilitada para la cámara. Seleccione la casilla de verificación para habilitar la generación de datos de movimiento de búsqueda inteligente en cámaras nuevas, cuando los añada al sistema con el asistente **Añadir hardware**. Este ajuste no afecta a los ajustes de detección de movimiento en las cámaras existentes. La generación de datos de movimiento de búsqueda inteligente para una cámara se habilita y deshabilita en la pestaña **Movimiento** para el dispositivo de cámara.
Al añadir dispositivos de cámaras nuevos, automáticamente se habilita: **Multidifusión**	Seleccione la casilla de verificación para habilitar la multidifusión en las cámaras nuevas cuando las añada con el asistente **Añadir hardware**. Este ajuste no afecta a los ajustes de multidifusión en las cámaras existentes.

Nombre	Descripción
	La multidifusión para una cámara se habilita y deshabilita en la pestaña **Cliente** para los dispositivos de cámaras.
Idioma	Seleccione el idioma de Management Client. Reinicie el Management Client para usar el nuevo idioma.
Permitir conexión no segura al servidor	Seleccione la casilla de verificación para permitir la conexión del servidor no segura mediante protocolo HTTP. (No se pide a ningún usuario que permita conexiones no seguras con el servidor). reinicie el Management Client para usar este ajuste.

Servidor de grabación

Nombre	Descripción
Tiempo de espera para sesiones PTZ manuales	Los usuarios del cliente con los permisos de usuario necesarios pueden interrumpir manualmente el patrullaje de las cámaras PTZ. Seleccione cuánto tiempo debe pasar antes de que se reanude la vigilancia regular después de la interrupción manual. El ajuste se aplica a todas las cámaras PTZ de su sistema. El ajuste predeterminado es 15 segundos. Si quiere tiempos de espera individuales en las cámaras, especifíquelo en la pestaña **Valores preestablecidos** para la cámara.
Tiempo de espera para pausar sesiones de vigilancia	Los usuarios clientes con una prioridad PTZ suficiente pueden pausar la vigilancia en las cámaras PTZ. Seleccione cuánto tiempo debe pasar antes de reanudar la vigilancia regular después de una pausa. El ajuste se aplica a todas las cámaras PTZ de su sistema. El ajuste predeterminado es 10 minutos. Si quiere tiempos de espera individuales en las cámaras, especifíquelo en la pestaña **Valores preestablecidos** para la cámara.
Tiempo de espera para sesiones PTZ	Establezca el periodo de tiempo de espera predeterminado para sesiones de PTZ reservadas. Cuando un usuario ejecuta una sesión PTZ reservada, la cámara PTZ

Nombre	Descripción
reservadas	no pueden usarla otros antes de que se libere manualmente o cuando se haya agotado el tiempo. El ajuste predeterminado es 1 hora. Si quiere tiempos de espera individuales en las cámaras, especifíquelo en la pestaña **Valores preestablecidos** para la cámara.
Utilizar valor preestablecido como posición de inicio de Pan/Tilt/Zoom	Seleccione esta casilla para utilizar la posición prestablecida de forma predeterminada en lugar de la posición de inicio de las cámaras PTZ al activar el botón **Inicio** en un cliente. Se debe definir una posición prestablecida para la cámara. Si no se define una posición prestablecida, no ocurrirá nada al activar el botón **Inicio** en un cliente. De forma predeterminada, esta casilla de verificación está desmarcada. Para asignar una posición prestablecida predeterminada, consulte Asignar la posición prestablecida de una cámara como predeterminada en la página 252
Ignore los errores de comunicación del dispositivo si la comunicación se reestablece antes	El sistema registra todos los errores de comunicación en el hardware y los dispositivos, pero aquí selecciona el tiempo que debe existir un error de comunicación antes de que la regla desencadene el evento **Error de comunicaicón**.

Pestaña Registros del servidor (opciones)

En la pestaña **Registros del servidor**, puede especificar los ajustes para los registros de servidores de gestión del sistema.

Para obtener más información, consulte Identificar actividad del usuario, eventos, acciones y errores.

Nombre	Descripción
Registros	Seleccione el tipo de registro que quiere configurar: • Registros del sistema • Registros de auditoría

Nombre	Descripción
	• Registros activados por reglas
Ajustes	Deshabilite o habilite los registros y especifique el periodo de retención. Permita que componentes 2018 R2 y anteriores escriban registros. Para obtener más información, consulte Permitir que 2018 R2 y componentes más antiguos escriban registros. Para registros del **sistema**, especifique el nivel de mensajes que quiere registrar: • Todo (incluye mensajes no definidos) • Información, advertencias y errores • Advertencias y errores • Errores (ajuste predeterminado) Para registros de **Auditoría**, habilite el registro del acceso de usuarios si quiere que el sistema registre todas las acciones de los usuarios en XProtect Smart Client. Estos son, por ejemplo, exportaciones, activación de salidas y visualización de cámaras en directo o en reproducción. Especificar: • La longitud de una secuencia de reproducción Esto significa que mientras que el usuario reproduce en este periodo, el sistema solo genera una entrada de registro. Al reproducir fuera del periodo, el sistema crea una nueva entrada de registro. • El número de registros (fotogramas) que ha visto un usuario antes de que el sistema cree una entrada de registro

Pestaña Servidor de correo (opciones)

En la pestaña **Servidor de correo**, puede especificar los ajustes para el servidor de correo de su sistema. Para obtener más información, consulte Perfiles de notificación (explicación).

Nombre	Descripción
Dirección de correo electrónico del remitente	Introduzca la dirección de correo electrónico que quiere que aparezca como remitente de notificaciones de correo electrónico para todos los perfiles de notificación. Ejemplo: **remitente@organización.org**.
Dirección del servidor de correo	Introduzca la dirección del servidor de correo SMTP que envía notificaciones por correo electrónico. Ejemplo: **servidordecorreo.organización.org**.
Puerto del servidor de correo	El puerto TCP utilizado para conectar con el servidor de correo. El puerto predeterminado es 25 para conexiones encriptadas; las conexiones encriptadas suelen usar el puerto 465 o 587.
Cifre la conexión con el servidor:	Si quiere asegurar la comunicación entre el servidor de gestión y el servidor de correo SMTP, seleccione esta casilla de verificación. La conexión se protege utilizando el comando STARTTLS del protocolo de correo electrónico. En este modo, la sesión se inicia en una conexión no cifrada, después el servidor de correo SMTP emite un comando STARTTLS al servidor de gestión para cambiar a una comunicación segura mediante SSL.
El servidor requiere datos de conexión	Si está habilitado, debe especificar un nombre de usuario y una contraseña para que el usuario inicie sesión en el servidor de correo.

Pestaña Generación de AVI (opciones)

En la pestaña **Generación de AVI**, puede especificar los ajustes de compresión para la generación de archivos de videoclips AVI. Los ajustes son necesarios si quiere incluir archivos AVI en notificaciones de correo electrónico enviadas por perfiles de notificación desencadenados por reglas.

Consulte también Desencadenar notificaciones de correo electrónico a partir de reglas.

Nombre	Descripción
Compresor	Seleccione el códec (tecnología de compresión/(descompresión) que quiera aplicar. Para que haya más códecs disponibles en la lista, instálelos en el servidor de gestión. No todas las cámaras admiten todos los códecs.
Calidad de compresión	(No disponible para todos los codecs). Utilice el control deslizante para seleccionar el grado de compresión (**0**-**100**) que debe realizar el códec. **0** significa la ausencia de compresión, que, por lo general, provoca una imagen de gran calidad y un tamaño de archivo grande. **100** significa la compresión máxima, que, por lo general, provoca una calidad de imagen baja y un tamaño de archivo pequeño. Si el control deslizante no está disponible, la calidad de compresión viene determinada enteramente por el códec seleccionado.
Fotograma clave cada	(No disponible para todos los codecs). Si quiere utilizar fotogramas clave, seleccione la casilla de verificación y especifique el número requerido de fotogramas entre fotogramas clave. UN fotograma clave es un único fotograma almacenado a intervalos especificados. El fotograma clave contiene la vista entera de la cámara, independientemente de si los siguientes fotogramas contienen solo los píxeles que cambian. Esto ayuda a reducir enormemente el tamaño de los archivos. Si la casilla de verificación no está disponible o no está seleccionada, cada fotograma contiene la vista entera de la cámara.
Tasa de datos	(No disponible para todos los codecs). Si quiere utilizar una velocidad de datos concreta, 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 está seleccionada la velocidad de los datos viene determinada por el códec seleccionado.

Pestaña Red (opciones)

En la pestaña **Red**, puede especificar las direcciones IP de los clientes locales, si los clientes van a conectarse al servidor de grabación por Internet. El sistema de vigilancia los reconoce entonces como procedentes de la red local.

También puede especificar la versión IP del sistema: IPv4 o IPv6. El valor predeterminado es IPv4.

Pestaña Marcador (opciones)

La funcionalidad disponible depende del sistema que esté utilizando. Vea la lista completa de características, que está disponible en la página de descripción del producto en el sitio web Milestone (https://www.milestonesys.com/solutions/platform/product-index/).

En la pestaña **Marcadores**, puede especificar ajustes para marcadores, sus ID y función en XProtect Smart Client.

Nombre	Descripción
Prefijo de ID de marcador	Especifique un prefijo para todos los marcadores creados por los usuarios de XProtect Smart Client.
Hora predeterminada del marcador	Especifique la hora de inicio y parada predeterminadas de un marcador que se establece en XProtect Smart Client. Este ajuste debe estar en consonancia con: • La regla de marcador predeterminada, consulte Reglas (nodo Reglas y Eventos). • El periodo previo al búfer para cada cámara, consulte Gestionar periodo previo al búfer.

Para especificar los permisos de marcadores de un cometido, consulte Pestaña Dispositivo (roles) en la página 573.

Pestaña Ajustes de usuario (opciones)

En la pestaña **Ajustes de usuario**, puede especificar ajustes de preferencia de usuarios, por ejemplo, si un mensaje debe mostrarse cuando la grabación remota está habilitada.

Pestaña IDP externo (opciones)

En la pestaña **IDP externo** en Management Client, puede añadir y configurar un IDP externo y registrar reclamaciones desde el IDP externo.

Nombre	Descripción
Habilitado	El IDP externo está habilitado por defecto.
Nombre	El nombre para el IDP externo. El nombre que introduzca aquí aparecerá en el campo **Autenticación** de la ventana de inicio de sesión de su cliente.
Autoridad de autentificación	El URL del IDP externo.
Añadir	Añada y configure un IDP externo. Cuando seleccione **Añadir**, se abrirá el cuadro de diálogo **IDP externo** y podrá introducir la información para la configuración, consulte **Configurar un IDP externo** debajo de la tabla.
Editar	Edite la configuración del IDP externo.
Borrar	Elimine la configuración del IDP externo.  Si quita una configuración de IDP externo, los usuarios que se autentifiquen a través de este IDP externo no podrán iniciar sesión en el VMS XProtect. Si vuelve a añadir el IDP externo, se crearán nuevos usuarios al iniciar sesión porque el ID del IDP externo ha cambiado.

Configurar un IDP externo

- Para añadir un IDP externo, seleccione **Añadir** en la sección **IDP externo** e introduzca la información de la tabla siguiente:

Nombre	Descripción
Nombre	El nombre para el IDP externo que introduzca aquí aparecerá en el campo **Autenticación** de la ventana de inicio de sesión de su cliente.
ID de cliente y **Secreto de cliente**	Debe obtenerse del IDP externo. El ID del cliente y el secreto del cliente son necesarios para comunicarse de forma segura con el IDP externo.

Nombre	Descripción
Ruta de retorno de llamada	Parte de una URL para el flujo de redirección de la autentificación para el registro de los usuarios. Los usuarios inician sesión desde una página de inicio de sesión alojada por el IDP externo. Cuando se completa el proceso de autenticación, se invoca esta ruta y se redirige al usuario al VMS XProtect. El valor por defecto es "/signin-oidc". El formato de redireccionamiento La URI de la ruta de devolución de llamada la crea el servidor de gestión FQID junto con /idp/ y la ruta de devolución de llamada configurada en el proveedor externo. Ejemplos: • Redireccionar formato URI para el XProtect Smart Client y el XProtect Management Client: [esquema]://[dirección del servidor de gestión]/idp/[ruta de devolución de llamada] • Redireccionar formato URI para el cliente XProtect Web Client y XProtect Mobile: [redireccionar Uri sin “/index.html”]/idp/[ruta de devolución de llamada] Tenga en cuenta que la parte "idp" de la ruta de devolución de llamada distingue entre mayúsculas y minúsculas y debe introducirse en minúsculas.
Solicitud de acceso	Especificar al IDP externo si el usuario debe permanecer conectado o si se requiere una verificación del usuario. Dependiendo del IDP externo, la verificación puede incluir una verificación de la contraseña o un inicio de sesión completo.
Reclamación a utilizar para crear el nombre de usuario	Opcionalmente, especifique qué reclamación del IDP externo que debe utilizarse para generar un nombre de usuario único para el usuario autoaprovisionado en el VMS. Para más información sobre los nombres de usuario únicos creados por las reclamaciones, consulte Nombres de usuario únicos para usuarios de IDP externo.
Ámbitos	Opcionalmente, utilice ámbitos para limitar el número de reclamaciones que recibe de un IDP externo. Si sabe que las reclamaciones que son relevantes para su VMS se encuentran en un ámbito específico, puede utilizar el ámbito para limitar el número de reclamaciones que obtiene del IDP externo.

Registrar reclamaciones

Cuando haya registrado las reclamaciones desde el IDP externo, podrá asignar las reclamaciones a los cometidos en el VMS para determinar los privilegios de los usuarios en el VMS. Para obtener más información, consulte Asignar reclamaciones desde un IDP externo.

- Para registrar reclamaciones de un IDP externo, seleccione **Añadir** en la sección **Reclamaciones registradas** e introduzca la información en la tabla siguiente:

Nombre	Descripción
IDP externo	El nombre del IDP externo.
Nombre de la reclamación	Nombre de la reclamación en texto libre. El nombre estará disponible al seleccionar un cometido.
Nombre de pantalla	El nombre de visualización de una reclamación.
Distingue entre mayús. y minús.	Indica si el valor de una reclamación distingue entre mayúsculas y minúsculas. Ejemplos de valores que suelen distinguir entre mayúsculas y minúsculas: - Representaciones textuales de los ID, como una guía: F951B1F0-2FED-48F7-88D3-49EB5999C923 o OadFgrDesdFesff= Ejemplos de valores que no suelen distinguir entre mayúsculas y minúsculas: - Direcciones de correo electrónico - Nombres de los cometidos - Nombres de grupos .
Añadir, **Editar**, **Eliminar**	Registrar y mantener reclamaciones. Si modifica una reclamación en el sitio web de IDP externo, los usuarios requieren un inicio de sesión de nuevo en el cliente XProtect. Digamos que un usuario, Bob, necesita ser, por ejemplo, Operador. La reclamación se añade entonces a Bob en el sitio web de IDP externo, pero si Bob ya ha iniciado sesión en XProtect, deberá completar un nuevo inicio de sesión para que el cambio surta efecto.

Añadir URI de redireccionamiento para los clientes web

El URI de redireccionamiento es la ubicación a la que se redirige al usuario después de iniciar sesión correctamente. Los URI de redireccionamiento deben ser una coincidencia exacta de las direcciones de los clientes web. Por ejemplo, no podrá iniciar sesión mediante un IDP externo si abre XProtect Web Client desde **https://localhost:8082/index.html** y el URI de redireccionamiento para los clientes web que añadió es **https://127.0.0.1:8082/index.html**.

Nombre	Descripción
URI	El URI de XProtect Web Client con el formato **https://[servidor móvil]:[puerto]/index.html**. Los URI de redireccionamiento no distinguen entre mayúsculas y minúsculas.
Añadir, **Editar**, **Eliminar**	Registre y mantenga los URI de redireccionamiento. Al eliminar los URI, debe conservar al menos un URI de redireccionamiento para que el sistema funcione.

Pestaña Panel de control del cliente (opciones)

En la pestaña **Panel del cliente**, puede habilitar o deshabilitar Milestone Customer Dashboard.

Panel de control del cliente es un servicio de monitorización en línea que proporciona una descripción gráfica del estado actual de su sistema, incluidos posibles problemas técnicos, como fallos de la cámara, a los administradores del sistema u otras personas a las que se les ha dado acceso a la información sobre la instalación de su sistema.

Puede seleccionar o desactivar la casilla de verificación para cambiar los ajustes del Panel del cliente en cualquier momento.

Pestaña Bloqueo de evidencias (opciones)

La funcionalidad disponible depende del sistema que esté utilizando. Vea la lista completa de características, que está disponible en la página de descripción del producto en el sitio web Milestone (https://www.milestonesys.com/solutions/platform/product-index/).

En la pestaña **Bloqueo de evidencias**, define y edita perfiles de bloqueo de evidencias y la duración que sus usuarios clientes pueden seleccionar para mantener protegidos los datos.

Nombre	Descripción
Perfiles de bloqueo de evidencias	Una lista con perfiles de bloqueos de evidencias definidos. Puede añadir o quitar perfiles de bloqueos de evidencias existentes. No puede eliminar el perfil del bloqueo de evidencias predeterminado, pero puede cambiar sus opciones de tiempo y su nombre.
Bloquear opciones de tiempo	La duración que los usuarios clientes pueden seleccionar para bloquear evidencias. Las opciones de tiempo disponibles son hora(s), día(s), semana(s), mes(es), año(s), indefinido o definido por el usuario.

Para especificar los permisos de acceso al bloqueo de evidencias de un cometido, consulte la Pestaña Dispositivo (roles) en la página 573 para los ajustes de los cometidos.

Pestaña Mensajes de audio (opciones)

En la pestaña **Mensajes de audio**, puede cargar archivos con mensajes de audio que se utilizan para transmitir mensajes desencadenados por reglas.

El número máximo de archivos cargados es 50 y el tamaño máximo permitido para cada archivo es 1 MB.

Nombre	Descripción
Nombre	Proporciona el nombre de un mensaje. El nombre se introduce al añadir un mensaje. Para cargar un mensaje en el sistema, haga clic en **Añadir**.
Descripción	Proporciona una descripción del mensaje. La descripción se alade al añadir un mensaje. Puede utilizar el campo de descripción para describir la finalidad o el mensaje real.
Añadir	Le permite cargar mensajes de audio en el sistema. Los formatos compatibles con formatos de archivos de audio estándar de Windows: • .wav • .wma

Nombre	Descripción
	• .flac
Editar	Le permite modificar el nombre y la descripción o puede sustituir el archivo real.
Borrar	Elimine el mensaje de audio de la lista.
Reproducir	Haga clic en este botón para escuchar el mensaje de audio desde el ordenador que ejecuta Management Client.

Para crear una regla que desencadene la reproducción de mensajes de audio, consulte Añadir una regla.

Para aprender más sobre acciones en general que puede usar en reglas, consulte Acciones y acciones de parada.

Pestaña Ajustes de privacidad

En la pestaña **Ajustes de privacidad**, puede habilitar o deshabilitar la recogida de datos de uso en XProtect Mobile Server, el cliente de XProtect Mobile, XProtect Web Client y XProtect Smart Client. A continuación, haga clic en **Aceptar**.

Al habilitar la recopilación de datos de uso, da su consentimiento para que Milestone Systems utilice tecnología de Google como un proveedor externo, con el que el procesamiento de datos en EE.UU. no se puede excluir. Para obtener más información sobre la protección de datos y la recopilación de datos de uso, consulte la guía de privacidad del RGPD.

Pestaña Ajustes de control de acceso (opciones)

El uso de XProtect Access requiere que haya adquirido una licencia básica que le permita acceder a esta característica.

Nombre	Descripción
Mostrar el panel de propiedades del desarrollo	Si se selecciona, aparece información adicional del desarrollador para **Control de acceso** > **Ajustes generales**. Este ajuste solo está destinado a su uso por parte de desarrolladores de integraciones de sistemas de control de acceso.

Pestaña Eventos de análisis (opciones)

En la pestaña **Eventos de análisis**, puede habilitar y especificar la función eventos de análisis.

Nombre	Descripción
Habilitar	Especifique si quiere utilizar eventos de análisis. De forma predeterminada, la característica está deshabilitada.
Puerto	Especifique el puerto utilizado por esta función. El puerto predeterminado es 9090. Asegúrese de que los proveedores de herramientas VCA relevantes también utilizan este número de puerto. Si cambia el número de puerto, recuerde cambiar el número de puerto de los proveedores.
Todas las direcciones de red o **Direcciones de red especificadas**	Especifique si los eventos de todas las direcciones IP/los nombres de host se permiten, o solo los eventos de direcciones IP/nombres de host que se especifiquen en la **lista de Direcciones** (consulte a continuación).
Lista de direcciones	Especifique una lista de direcciones IP/nombres de host de confianza. La lista filtra los datos entrantes de modo que solo los eventos de ciertas direcciones IP/nombres de host estén permitidos. Puede utilizar tanto formatos de dirección tanto IPv4 como IPv6 en el Sistema de Nombres de Dominio (Domain Name System, DNS). Puede añadir direcciones a su lista introduciendo manualmente cada dirección IP o nombre de host, p importando una lista externa de direcciones.

Nombre	Descripción
	• **Introducción manual**: Introduzca la dirección IP/nombre de host en la lista de direcciones. Repetir para cada dirección requerida • **Importar**: 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

Pestaña Alarmas y eventos (opciones)

En la pestaña **Alarmas y eventos**, puede especificar ajustes para alarmas, eventos y registros. En relación con estos, consulte también Limitar el tamaño de la base de datos en la página 133.

Nombre	Descripción
Mantener las alarmas cerradas durante	Especifique el número de días para almacenar alarmas con el estado **Cerrado** en la base de datos. Si establece el valor en **0**, la alarma se elimina después de haberla cerrado.  Las alarmas siempre tienen marcas de tiempo. Si la alarma la desencadena una cámara, la marca de tiempo tiene una imagen de la hora de la alarma. La propia información de la alarma 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 relevante. Para poder ver las imágenes de sus alarmas, conserve las grabaciones de vídeo al menos mientras tenga intención de conservar las alarmas en el servidor de eventos.
Mantener todas las demás alarmas durante	Especifique el número de días para almacenar alarmas con el estado **Nueva**, **En curso** o **En espera**. Si establece el valor en 0, la alarma aparece en el sistema, pero no se almacenará.

Nombre	Descripción
	 Las alarmas siempre tienen marcas de tiempo. Si la alarma la desencadena una cámara, la marca de tiempo tiene una imagen de la hora de la alarma. La propia información de la alarma 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 relevante. Para poder ver las imágenes de sus alarmas, conserve las grabaciones de vídeo al menos mientras tenga intención de conservar las alarmas en el servidor de eventos.
Mantener registros durante	Especifique el número de días para mantener los registros del servidor de eventos. Si conserva los registros durante periodos de tiempo más largos, asegúrese de que la máquina en la que está instalado el servidor de eventos tiene suficiente espacio en el disco.
Activar registro detallado	Para conservar un registro más detallado para la comunicación con el servidor de eventos, seleccione la casilla de verificación. Se almacenará durante el número de días especificado en el campo **Mantener registros durante**.
Tipos de evento	Especifique el número de días para almacenar eventos en la base de datos. Hay dos formas de hacerlo: • Puede especificar el tiempo de retención para todo el grupo de eventos. Los tipos de evento con el valor **Seguir 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.

Nombre	Descripción
	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. El motivo es que estos tipos de eventos se producen con tanta frecuencia que almacenarlos en la base de datos puede causar problemas de rendimiento.

Pestaña Eventos genéricos (opciones)

En la pestaña **Eventos genéricos**, puede especificar ajustes relacionados con fuentes de datos y eventos genéricos.

Para obtener más información sobre cómo configurar eventos genéricos reales, consulte Eventos genéricos (explicación).

Nombre	Descripción
Fuente de datos	Puede elegir entre dos fuentes de datos predeterminadas y definir una fuente de datos personalizada. Lo que elija depende de su programa de terceros y/o del hardware o software desde el que quiera interactuar: **Compatible**: Los ajustes predeterminados de fábrica están habilitados, refleja todos los bytes, TCP y UDP, solo IPv4, puerto 1234, sin separador, solo host local, codificación de página de códigos actual (ANSI). **Internacional**: Los ajustes predeterminados de fábrica están habilitados, refleja solo estadísticas, solo TCP, IPv4+6, puerto 1235, <CR><LF> como separador, solo host local, codificación UTF-8. (<CR><LF> = 13,10). [Fuente de datos A] [Fuente de datos B] etc.
Nuevo	Haga clic para definir una nueva fuente de datos.

Nombre	Descripción
Nombre	Nombre de la fuente de datos.
Habilitado	Las fuentes de datos están habilitadas de forma predeterminada. Desactive la casilla de verificación para deshabilitar la fuente de datos.
Reiniciar	Haga clic para restablecer todos los ajustes para la fuente de datos seleccionada. El nombre introducido en el campo **Nombre** se mantiene.
Puerto	El número de puerto de la fuente de datos.
Selector del tipo de protocolo	Los protocolos a los que debe escuchar el sistema, y analizar, con el fin de detectar eventos genéricos: **Cualquiera**: TCP así como UDP. **TCP**: Solo TCP. **UDP**: Solo UDP. Los paquetes TCP y UDP utilizados para eventos genéricos pueden contener caracteres especiales, como @, #, +, ~ y más.
Selector de tipo de IP	Tipos de dirección IP seleccionables: IPv4, IPv6 o ambos.
Bytes de separador	Seleccione los bytes separadores utilizados para separar registros de eventos genéricos individuales. El valor pPredeterminado para el tipo de fuente de datos **Internacional** (consulte **Fuentes de datos** previamente) es **13,10**. (13,10 = <CR><IF>).
Reflejar tipo de selector	Formatos de retorno de eco disponible: • **Reflejar estadísticas**: Refleja el siguiente formato: **[X],[Y],[Z],[Nombre de evento genérico]** **[X]** = número de solicitud. **[Y]** = número de caracteres. **[Z]** = número de coincidencias con un evento genérico. **[Nombre de evento genérico]** = nombre introducido en el campo **Nombre**. • **Reflejar todos los bytes**: Refleja todos los bytes

Nombre	Descripción
	• **Sin eco**: Suprime todo el eco
Selector del tipo de codificación	De forma predeterminada. la lista solo muestra las opciones más relevantes. Seleccione la casilla de verificación **Mostrar todo** para mostrar todas las codificaciones disponibles.
Direcciones IPv4 externas permitidas	Especifique las direcciones IP con las que el servidor de gestión debe comunicarse para gestionar eventos externos. También puede usar esto para excluir direcciones IP de las que no quiere datos.
Direcciones IPv6 externas permitidas	Especifique las direcciones IP con las que el servidor de gestión debe comunicarse para gestionar eventos externos. También puede usar esto para excluir direcciones IP de las que no quiere datos.

Menús de componentes

Management Client menús

Menú Archivo

Puede guardar los cambios en la configuración y salir de la aplicación. También puede hacer una copia de seguridad de su configuración, consulte Hacer una copia de seguridad y restaurar la configuración del sistema (explicación) en la página 340.

Editar menú

Puede deshacer los cambios.

Menú Ver

Nombre	Descripción
Restablecer distribución de la interfaz	Restablezca el diseño de los distintos paneles en Management Client a sus ajustes predeterminados.

Nombre	Descripción
Ventana de previsualización	Active y desactive el panel **Vista previa** cuando trabaje con dispositivos y servidores de grabación.
Mostrar flujos de grabación	De forma predeterminada, la información que se muestra con imágenes de vista previa en el panel **Vista previa** afecta a flujos en directo de las cámaras. Si, por el contrario, quiere información sobre flujos de grabación, seleccione **Mostrar flujos de grabación**.
Jerarquía de sitios federados	De forma predeterminada, el panel **Jerarquía de sitios federados** está habilitado.
Navegación del sitio	De forma predeterminada, el panel **Navegación por el sitio** está habilitado.

Menú Acción

El contenido del menú **Acción** difiere dependiendo del elemento que ha seleccionado en el panel **Navegación por el sitio**. Las acciones entre las que puede elegir son las mismas que cuando hace clic con el botón derecho en el elemento.

El periodo previo al búfer para cada cámara, consulte Gestionar periodo previo al búfer.

Nombre	Descripción
Actualizar	Siempre está disponible y recarga la información requerida del servidor de gestión.

Menú de herramientas

Nombre	Descripción
Servicios registrados	Gestione servicios registrados. Consulte Gestión de los servicios registrados en la página 370.
Roles efectivos	Vea todos los roles de un usuario o grupo seleccionado.

Nombre	Descripción
Opciones	Abre el cuadro de diálogo Opciones, que le permite definir y editar ajustes del sistema global. Si desea más información, consulte Ajustes del sistema (cuadro de diálogo Opciones) en la página 396.

Menú Ayuda

Puede acceder al sistema de ayuda y a información sobre la versión de Management Client.

Server Configurator (Utilidad)

Propiedades de la pestaña Encriptación

Esta pestaña le permite especificar las siguientes propiedades:

En un entorno de clúster, debe configurar su clúster y asegurarse de que se está ejecutando antes de crear certificados para todos los ordenadores en el entorno del clúster. Después de eso, puede instalar los certificados y hacer el registro utilizando Server Configurator para todos los nodos del clúster. Si desea más información, consulte la guía de certificados sobre cómo asegurar sus instalaciones XProtect VMS.

Nombre	Descripción	Tarea
Certificado del servidor	Seleccione el certificado que se utilizará para cifrar la conexión de dos direcciones entre el servidor de gestión, los colectores de datos, el servidor de registro y los servidores de grabación.	Habilitar encriptación en y desde el servidor de gestión Habilitar encriptación del servidor para los servidores de grabación o los servidores remotos
Servidor de eventos y add-ons	Seleccione el certificado que se utilizará para cifrar la conexión bidireccional entre el servidor de eventos y los componentes que se comunican con el servidor de eventos, incluido el LPR Server.	Habilitar el cifrado del servidor de eventos en la página 313

Nombre	Descripción	Tarea
Certificado de medios de transmisión	Seleccione el certificado que se utilizará para cifrar la comunicación entre los servidores de grabación y todos los clientes, servidores e integraciones que recuperan flujos de datos de los servidores de grabación.	Habilitar encriptación en clientes y servidores
Certificado de medios de transmisión móvil	Seleccione el certificado que se utilizará para cifrar la comunicación entre el servidor móvil y los clientes móviles y web que recuperan flujos de datos del servidor móvil.	Habilitar encriptación en el servidor móvil

Servidores de registro

Nombre	Descripción	Tarea
Dirección del servidor de gestión	La dirección del servidor de gestión normalmente incluye el nombre de host o el nombre de dominio totalmente cualificado (fully qualified domain name, FQDN) del ordenador. De forma predeterminada, esta dirección solo está activa en XProtect VMS en el que el servidor de gestión no está instalado. Como norma general, la dirección del servidor de gestión no debe cambiarse desde un ordenador que tiene instalado el servidor de gestión. Sin embargo, si, por ejemplo, utiliza el Server Configurator en una configuración de failover, podría tener que cambiar la dirección desde el ordenador del servidor de gestión. Esto podría estar dentro de un entorno de failover de clúster o en otro escenario de configuración de failover.	Haga clic en más información sobre las implicaciones de cambiar la dirección del servidor de gestión desde un ordenador que tiene instalado un servidor de gestión: Cambiar el nombre de host del ordenador del servidor de gestión

Nombre	Descripción	Tarea
	• Para activar el campo **Dirección del servidor de gestión** desde un ordenador con el servidor de gestión instalado, haga clic en el símbolo del lápiz (). Si actualiza la dirección del servidor de gestión, debe acceder a cada uno de los ordenadores que tienen componentes instalados y actualizar la dirección del servidor de gestión con la información de la nueva dirección.	
Registro	Registre los servidores que se están ejecutando en el ordenador con el servidor de gestión designado.	Registrar un servidor de grabación

Selección de idioma

Utilice esta pestaña para seleccionar el idioma para el Server Configurator. El conjunto de idiomas para el Server Configurator se corresponde con el conjunto de idiomas para el Management Client.

Nombre	Descripción
Elija un idioma	Elija el idioma de la interfaz de usuario.

Si trabaja en un entorno de clúster de failover, se recomienda poner en pausa el clúster antes de iniciar las tareas en el Server Configurator. Esto se debe a que Server Configurator puede ser necesario detener los servicios mientras se aplican los cambios y el entorno del clúster de failover puede interferir con esta operación.

Estado del icono de la bandeja

Los iconos de la bandeja de la tabla muestran los distintos estados de los servicios que se ejecutan en los servidores en XProtect VMS. Los iconos están disponibles en ordenadores con los servidores instalados:

Management Server Manager icono de bandeja	Recording Server Manager icono de bandeja	Event Server Manager icono de bandeja	Failover Recording Server Manager icono de bandeja	Descripción
				**Ejecutando** Aparece cuando se habilita e inicia un servicio de servidor. Si el servicio Failover Recording Server está funcionando, puede hacerse cargo si los servidores de grabación estándar fallan.
				**Detenido** Aparece cuando un servicio del servidor se ha detenido.

Management Server Manager icono de bandeja	Recording Server Manager icono de bandeja	Event Server Manager icono de bandeja	Failover Recording Server Manager icono de bandeja	Descripción
				Si el servicio Failover Recording Server se detiene, no puede hacerse cargo si los servidores de grabación estándar fallan.
				**Iniciando** Aparece cuando un servicio del servidor está en proceso de iniciarse. En circunstancias normales, el icono de la bandeja cambia al poco tiempo a **En ejecución**.
				**Deteniéndose** Aparece cuando un servicio del servidor está en proceso de detenerse. En circunstancias normales, el icono de la bandeja cambia al poco tiempo a **Detenido**.
				**En estado indeterminado**

Management Server Manager icono de bandeja	Recording Server Manager icono de bandeja	Event Server Manager icono de bandeja	Failover Recording Server Manager icono de bandeja	Descripción
				Aparece cuando el servicio del servidor se carga inicialmente y hasta que se recibe la primera información, tras lo cual el icono de la bandeja, en circunstancias normales, cambia a **Iniciando** y después a **En ejecución**.
				**Funcionamiento fuera de línea** Suele aparecer cuando el servidor de grabación o el servicio de grabación de failover está en funcionamiento pero el servicio Management Server no lo está.

Inicio y parada de servicios desde iconos de la bandeja

Haga clic con el botón derecho en los iconos en el área de notificación para abrir iconos de la bandeja en los que puede iniciar y detener servicios.

- Iniciar o detener el servicio Management Server
- Iniciar o detener el servicio Recording Server

Management Server Manager (icono de bandeja)

Utilice los elementos del menú en el icono de la bandeja de Management Server Manager para realizar tareas desde Management Server Manager.

Nombre	Descripción
Iniciar Management Server y **Parar Management Server**	Haga clic en el elemento del menú apropiado para iniciar o detener el servicio Management Server. Si detiene el servicio Management Server, no puede usar Management Client. El estado del servicio se ve reflejado por el icono de la bandeja. Para obtener información adicional sobre los estados de los iconos de la bandeja, consulte Iconos de la bandeja del gestor de servidores (explicación).
Mostrar mensajes de estado	Vea una lista de mensajes de estado con marca de tiempo.
Cambiar ajustes de contraseña de la configuración del sistema	Asigne o cambie una contraseña de configuración del sistema. También puede elegir no proteger con contraseña la configuración del sistema eliminando cualquier contraseña asignada para la configuración del sistema. Cambiar los ajustes de contraseña de la configuración del sistema
Introducir la contraseña de configuración del sistema	Introduzca una contraseña. Esto se aplica si, por ejemplo, el archivo que contiene los ajustes de la contraseña se elimina o si está dañado. Para obtener infomración adicional, consulte Entrar en los ajustes de configuración de configuración del sistema.
Configurar el servidor de gestión failover	Inicie el asistente de configuración del servidor de gestión de failover o abra la página **Gestionar su configuración** para gestionar la configuración existente. Para obtener más información sobre el clúster de conmutación por error, consulte XProtect Management Server Failover en la página 36.
Server Configurator	Abra **Server Configurator** para registrar servidores y gestionar la encriptación. Para obtener información adicional sobre la gestión de la encriptación, consulte Gestionar encriptación con Server Configurator.
Cambiar licencia	En el ordenador del servidor de gestión, cambie el código de la licencia del software. Necesitaría introducir un nuevo código de licencia para, por ejemplo, actualizar su sistema XProtect. Para obtener más información, consulte Cambiar el código de licencia del software.
Restaurar configuración	Abra un cuadro de diálogo desde el que puede restaurar la configuración del sistema. Asegúrese de leer la información del cuadro de diálogo antes de hacer

Nombre	Descripción
	clic en **Restaurar**. Para obtener información adicional, consulte Restaurar configuración del sistema de una copia de seguridad manual.
Seleccionar la carpeta de copia de seguridad compartida	Establezca una carpeta de copias de seguridad en la que almacenar su copia de seguridad antes de hacer la copia de seguridad de cualquier configuración del sistema. Para obtener información adicional, consulte Seleccionar carpeta de copia de seguridad compartida.
Actualizar dirección SQL	Abra un asistente para cambiar la dirección del SQL Server. En el caso poco frecuente de un cambio de nombre de host, la dirección de SQL Server podría necesitar ajustarse a los cambios. Para obtener información adicional, consulte Un cambio de nombre de host puede desencadenar el cambio de la dirección del servidor SQL.

Nodo básico

Información de licencias (nodo Aspectos básicos)

En la ventana de **Información de licencia**, puede llevar un registro de todas las licencias que comparten el mismo archivo de licencia de software tanto en este sitio como en todos los demás sitios, sus suscripciones de Milestone Care y decidir cómo quiere activar sus licencias.

Para saber más sobre las distintas informaciones y funciones disponibles en la ventana de **Información sobre licencia**, consulte Ventana de información de la licencia en la página 128.

Información del sitio (nodo Aspectos básicos)

En una configuración grande de Milestone Federated Architecture con muchos sitios secundarios, es fácil perder la visión de conjunto y puede ser difícil encontrar la información de contacto de los administradores de cada sitio secundario.

Por lo tanto, puede añadir información adicional a cada sitio secundario y esta información estará disponible para los administradores en el sitio central.

Es posible añadir la siguiente información:

- Nombre del sitio
- Dirección/ubicación
- Administrador(es)

- Información adicional

Nodo de servicios de conexión remota

Conexión de cámara Axis One-click (nodo Servicios de conexión remota)

Estas son las propiedades de conexión de la cámara Axis One-Click.

Nombre	Descripción
Contraseña de la cámara	Introduzca/edite. Se proporciona con la cámara al comprar. Para obtener más detalles, consulte el manual de su cámara o vaya al sitio web de Axis (https://www.axis.com/).
Usuario de la cámara	Consulte los detalles para **Contraseña de la cámara**.
Descripción	Introduzca/edite una descripción para la cámara.
Dirección externa	Introduzca/edite la dirección web del servidor ST al que se conectan las cámaras.
Dirección interna	Introduzca/edite la dirección web del servidor ST al que se conecta el servidor de grabación.
Nombre	En caso necesario, edite el nombre del elemento.
Clave de autenticación del propietario	Consulte **Contraseña de la cámara**.
Contraseñas (para Servidor de envío)	Introduzca la contraseña. Debe ser idéntico al recibido de su proveedor del sistema.
Contraseñas (para servidor ST)	Introduzca la contraseña. Debe ser idéntico al que introdujo cuando se instaló el componente Axis One-Click Connection.
Registrar/Anular registro en el servicio de envío Axis	Indique si desea registrar su cámara Axis con el servicio de envío Axis. Se puede hacer en el momento de la configuración o más adelante.

Nombre	Descripción
Número de serie	Número de serie de hardware según lo especificado por el fabricante. Con frecuencia, pero no siempre, el número de serie es idéntico a la dirección MAC.
Usar credenciales	Seleccione la casilla de verificación si ha decidido utilizar credenciales durante la instalación del servidor ST.
Nombre de usuario (para Servidor de envío)	Introduzca un nombre de usuario. El nombre del usuario debe ser idéntico al que se recibió de l proveedor del sistema.
Nombre de usuario (para servidor ST)	Introduzca el nombre de usuario. Debe ser idéntico al que introdujo cuando se instaló el **componente Axis One-Click Connection**.

Nodo de servidores

Servidores (nodo)

Esta sección describe cómo instalar y configurar servidores de grabación y servidores de grabación de failover. También aprende a añadir hardware nuevo al sistema y a interconectar otros sitios.

- Servidores de grabación (nodo Servidores) en la página 427
- Servidores de failover (nodo Servidores) en la página 441

Servidores de grabación (nodo Servidores)

El sistema utiliza servidores de grabación para grabar los flujos de vídeo y para comunicarse con las cámaras y otros dispositivos. Un sistema de vigilancia suele estar formado por varios servidores de grabación.

Los servidores de grabación son ordenadores en los que se ha instalado el software Recording Server y se ha configurado para que se comunique con el servidor de gestión. Podrá ver sus servidores de grabación en el panel de **Generalidades** cuando expanda la carpeta **Servidores** y luego seleccione **Servidores de grabación**.

La compatibilidad con versiones del servidor de grabación anteriores a esta versión del servidor de gestión es limitada. Puede seguir accediendo a las grabaciones de los servidores de grabación con versiones anteriores, pero si quiere cambiar su configuración, asegúrese de que coinciden con esta versión del servidor de gestión. Milestone recomienda que actualice todos los servidores de grabación de su sistema a la misma versión que el servidor de gestión.

Ventana Ajustes del servidor de grabaciones

Al hacer doble clic en el icono de la bandeja de Recording Server Manager y seleccionar **Cambiar ajustes**, puede especificar lo siguiente:

Nombre	Descripción
Dirección	Dirección IP (ejemplo: 123.123.123.123) o nombre de host (ejemplo: nuestroservidor) del servidor de gestión al que se debe conectar el servidor de grabación. Esta información es necesaria para que el servidor de grabación pueda comunicarse con el servidor de gestión.
Puerto	Número de puerto que se debe usar al comunicarse con el servidor de gestión. El valor predeterminado es el puerto 9000. Puede cambiar esto si fuera necesario.
Por tal del servidor web	Número de puerto que se va a usar para manejar solicitudes del servidor web, por ejemplo, para manejar comandos de control de la cámara PTZ y para explorar y solicitudes en directo desde XProtect Smart Client. El valor predeterminado es el puerto 7563. Puede cambiar esto si fuera necesario.
Puerto del servidor de alertas	Número de puerto que se debe usar cuando el servidor de grabación escucha información de TCP (algunos dispositivos utilizan TCP para enviar mensajes de eventos). El valor predeterminado es puerto 5432 (deshabilitado de forma predeterminada). Puede cambiarlo si lo necesita.
Puerto del servidor SMTP	Número de puerto que se debe usar cuando el servidor de grabaciones escucha información del Protocolo simple de transferencia de correo (Simple Mail Transfer Protocol, SMTP). SMTP es un estándar para enviar mensajes de correo electrónico entre servidores. Algunos dispositivos utilizan SMTP para enviar mensajes de eventos o imágenes al servidor del sistema de vigilancia por correo electrónico. El valor predeterminado es puerto 25, que puede habilitar y deshabilitar. Puede cambiar el número de puerto si lo necesita.
Encriptar	Antes de habilitar la encriptación y seleccionar un certificado de autenticación del

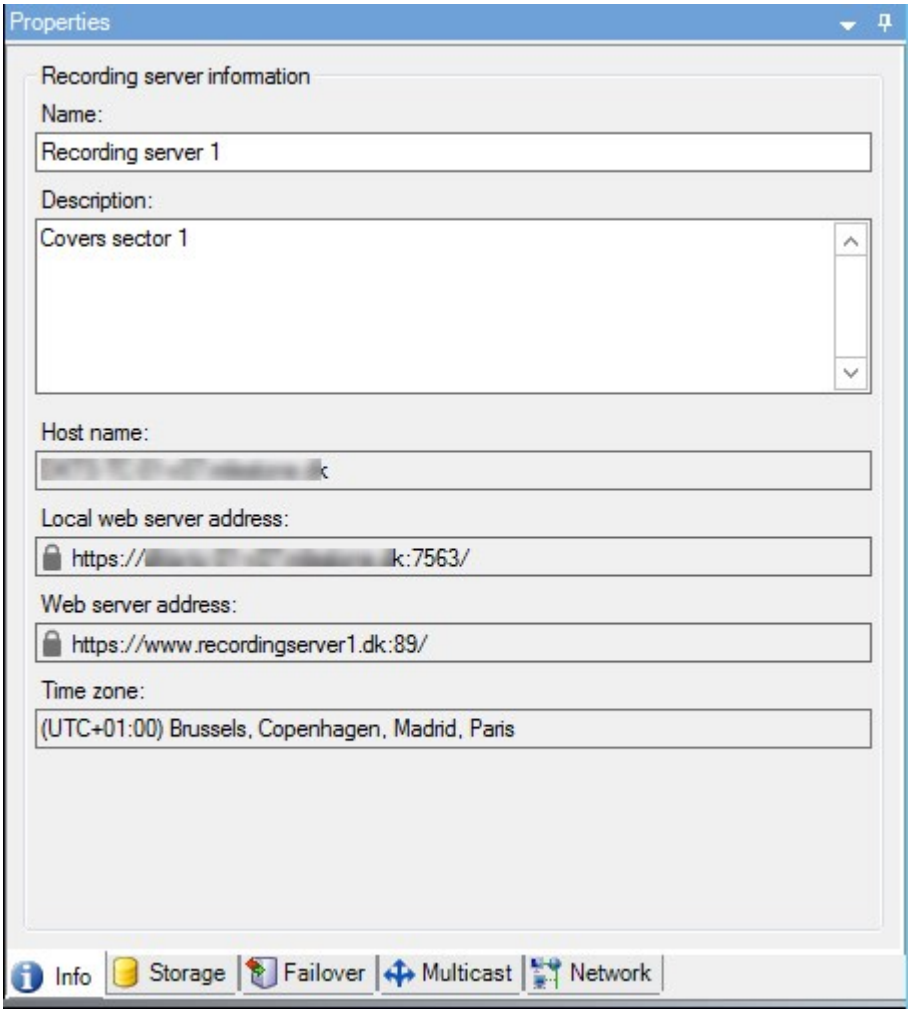
Nombre	Descripción
conexiones desde el servidor de gestión al servidor de grabación	servidor de la lista, asegúrese de que habilita la encriptación en el servidor de gestión primero y que el servidor de grabación confía en el certificado del servidor de grabación. Si desea más información, consulte Comunicación segura (explicación) en la página 150.
Encriptar conexiones a clientes y servicios que transmiten datos	Antes de habilitar la encriptación y seleccionar un certificado de autenticación del servidor de la lista, asegúrese de que todos los ordenadores confían en el certificado que ejecuten servicios que recuperan flujos de datos desde el servidor de grabación. XProtect Smart Client y todos los servicios que reciben flujos de datos del servicio de grabación deben estar actualizados a la versión 2019 R1 o posterior. Algunas soluciones de terceros creadas utilizando versiones de MIP SDK anteriores a la 2019 R1 pueden necesitar una actualización. Si desea más información, consulte Comunicación segura (explicación) en la página 150. Para verificar que su servidor de grabación utiliza encriptación, consulte Ver el estado del cifrado a los clientes en la página 299.
Detalles	Vea información sobre el certificado seleccionado en Almacenamiento de certificados en Windows.

Propiedades de servidores de grabación

Pestaña Información (servidor de grabación)

En la pestaña **Información**, puede verificar o editar el nombre y la descripción del servidor de grabación.

Puede ver el nombre de host y las direcciones. El icono del candado delante de la dirección del servidor web indica comunicación encriptada con los clientes y servicios que recuperan flujos de datos desde este servidor de grabación.



Nombre	Descripción
Nombre	Puede elegir introducir un nombre para el servidor de grabación. El nombre se utiliza en el sistema y los clientes cuando se aparece recogido el servidor de grabación. No es necesario que el nombre sea único. Cuando cambie el nombre de un servidor de grabación, el nombre cambia globalmente en Management Client.
Descripción	Puede elegir entre una descripción que aparece en un número de listados dentro del sistema. Una descripción no es obligatoria.
Nombre de	Muestra el nombre de host del servidor de grabación.

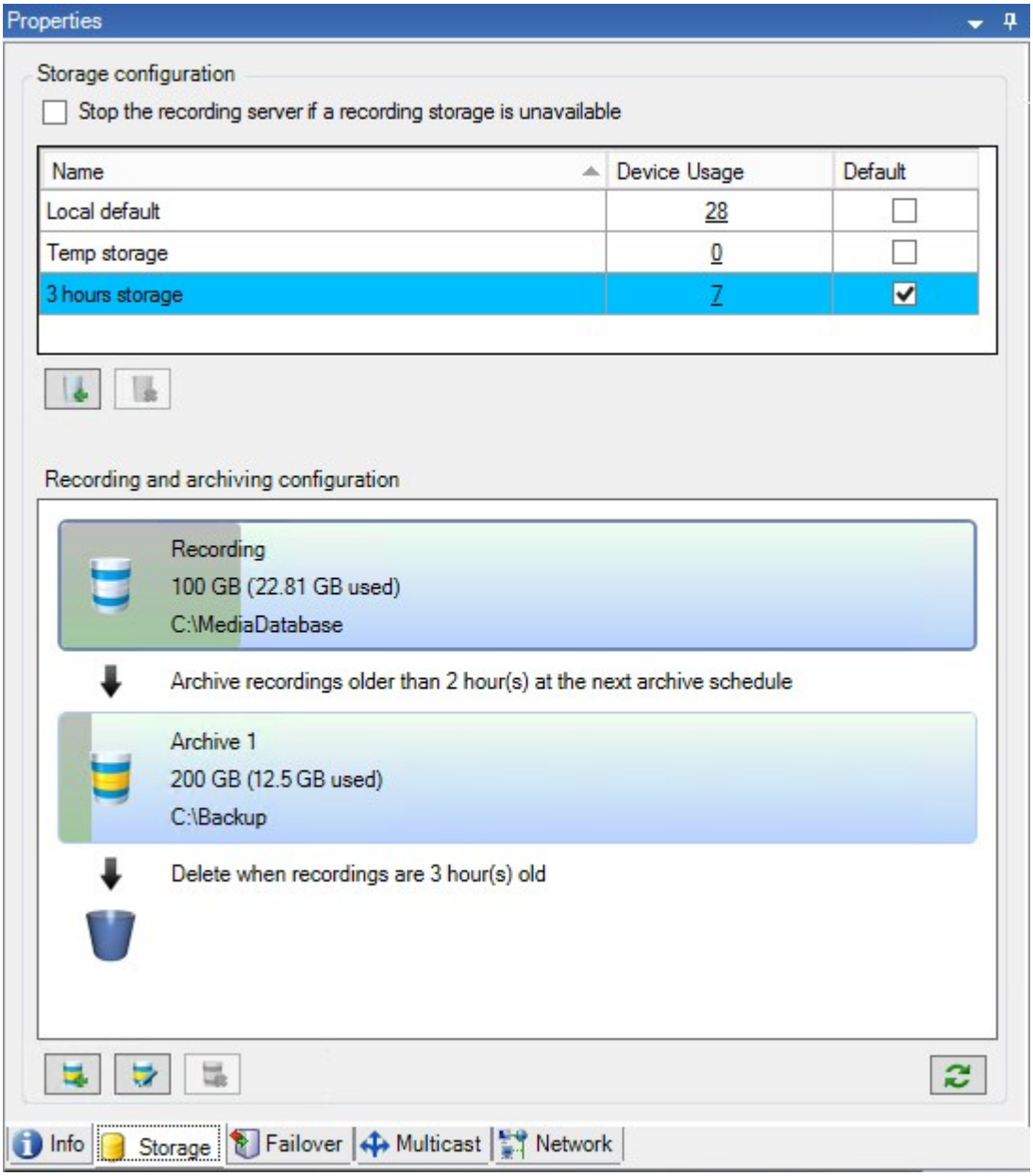
Nombre	Descripción
host	
Dirección del servidor web local	Muestra la dirección local del servidor web del servidor de grabación. Usted utiliza la dirección local, por ejemplo, para gestionar comandos de control de cámaras PTZ, y para gestionar la navegación y las solicitudes en directo desde XProtect Smart Client. La dirección incluye el número de puerto que se usa para la comunicación con el servidor web (normalmente puerto 7563). Si habilita la encriptación a clientes y servidores que recuperan flujos de datos del servidor de grabación, aparece el icono de un candado, y la dirección incluye **https** en lugar de **http**.
Dirección de servidor web	Muestra la dirección pública del servidor web del servidor de grabación en Internet. Si su instalación utiliza un cortafuegos o un router NAT, introduzca la dirección del cortafuegos o el router NAT de modo que los clientes que accedan al sistema de vigilancia en Internet se puedan conectar al servidor de grabación. Usted especifica la dirección pública y el número de puerto en la pestaña **Red**. Si habilita la encriptación a clientes y servidores que recuperan flujos de datos del servidor de grabación, aparece el icono de un candado, y la dirección incluye **https** en lugar de **http**.
Zona horaria	Muestra la zona horaria en la que está ubicado el servidor de grabación.

Pestaña Almacenamiento (servidor de grabación)

En la pestaña **Almacenamiento**, puede configurar, gestionar y ver los almacenamientos de un servidor de grabación seleccionado.

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

Si está utilizando el **Bloqueo de evidencias**, habrá una línea roja vertical que mostrará el espacio utilizado para las secuencias bloqueadas de evidencias.



Propiedades de Ajustes de almacenamiento y grabación

La funcionalidad disponible depende del sistema que esté utilizando. Vea la lista completa de características, que está disponible en la página de descripción del producto en el sitio web Milestone (https://www.milestonesys.com/solutions/platform/product-index/).

En el cuadro de diálogo **Ajustes de almacenamiento y grabación**, especifique lo siguiente:

Nombre	Descripción
Nombre	En caso necesario, cambie el nombre del almacenamiento. Los nombres deben ser únicos.
Ruta	Especifique la ruta al directorio en el que guarda grabaciones en este almacenamiento. El almacenamiento no necesariamente tiene que estar ubicado en el servidor de grabación. Si el directorio no existe, puede crearlo. Las unidades de red deben especificarse utilizando el formato UNC (Convención de Nomenclatura Universal, Universal Naming Convention), por ejemplo: `\\servidor\volumen\directorio\`.
Periodo de retención	Especifique durante cuánto tiempo deben permanecer las grabaciones en el archivo antes de que se eliminen o se muevan al siguiente archivo (dependiendo de los ajustes de archivo). El tiempo de retención siempre debe ser superior al tiempo de retención del archivo previo o la base de datos de grabación predeterminada. Esto se debe a que el número de días de retención especificado para un archivo incluye todos los periodos de retención indicados previamente en el proceso.
Tamaño máximo	Seleccione el número máximo de gigabytes de datos de grabación para guardar en la base de datos de grabaciones. La grabación de datos que supere el número especificado de gigabytes se mueve automáticamente al primer archivo de la lista - si se especifica alguno - o se elimina. ⚠ Cuando hay menos de 5 GB de espacio libre, el sistema siempre autoarchiva (o elimina si no se ha definido ningún próximo archivo) los datos más antiguos en una base de datos. Si hay menos de 1 GB de espacio libre, los datos se eliminan. Una base de datos siempre requiere 250 MB de espacio libre. Si alcanza este límite (si no se eliminan datos lo bastante rápido), no se escriben más datos en la base de datos hasta que haga liberado suficiente espacio. El tamaño máximo real de su base de datos es la cantidad de gigabytes que especifique, menos 5 GB.
Firma	Habilita una firma digital para las grabaciones. Esto significa, por ejemplo, que el sistema confirma que el vídeo exportado no se ha modificado o manipulado al reproducirlo.

Nombre	Descripción
	El sistema utiliza el algoritmo SHA-2 para la firma digital.
Cifrado	Seleccione el nivel de encriptación de las grabaciones: • Ninguno • Ligero (menos uso de la CPU) • Fuerte (más uso de la CPU) El sistema utiliza e algoritmo AES-256 para la encriptación. Si selecciona **Ligera**, una parte de la grabación está encriptada. Si selecciona **Fuerte**, toda la grabación se encripta. SI opta por habilitar la encriptación, también debe especificar una contraseña a continuación.
Contraseña	Introduzca una contraseña para los usuarios a los que se permita ver datos encriptados. Milestone recomienda que utilice contraseñas fuertes. Las contraseñas potentes no contienen palabras que puedan encontrarse en un diccionario ni son parte del nombre del usuario. Incluyen ocho o más caracteres alfanuméricos, mayúsculas y minúsculas, y caracteres especiales.

Propiedades de ajustes de archivo

En el cuadro de diálogo **Ajustes de archivo**, especifique lo siguiente:

Nombre	Descripción
Nombre	En caso necesario, cambie el nombre del almacenamiento. Los nombres deben ser únicos.
Ruta	Especifique la ruta al directorio en el que guarda grabaciones en este almacenamiento. El almacenamiento no necesariamente tiene que estar ubicado en el servidor de grabación.

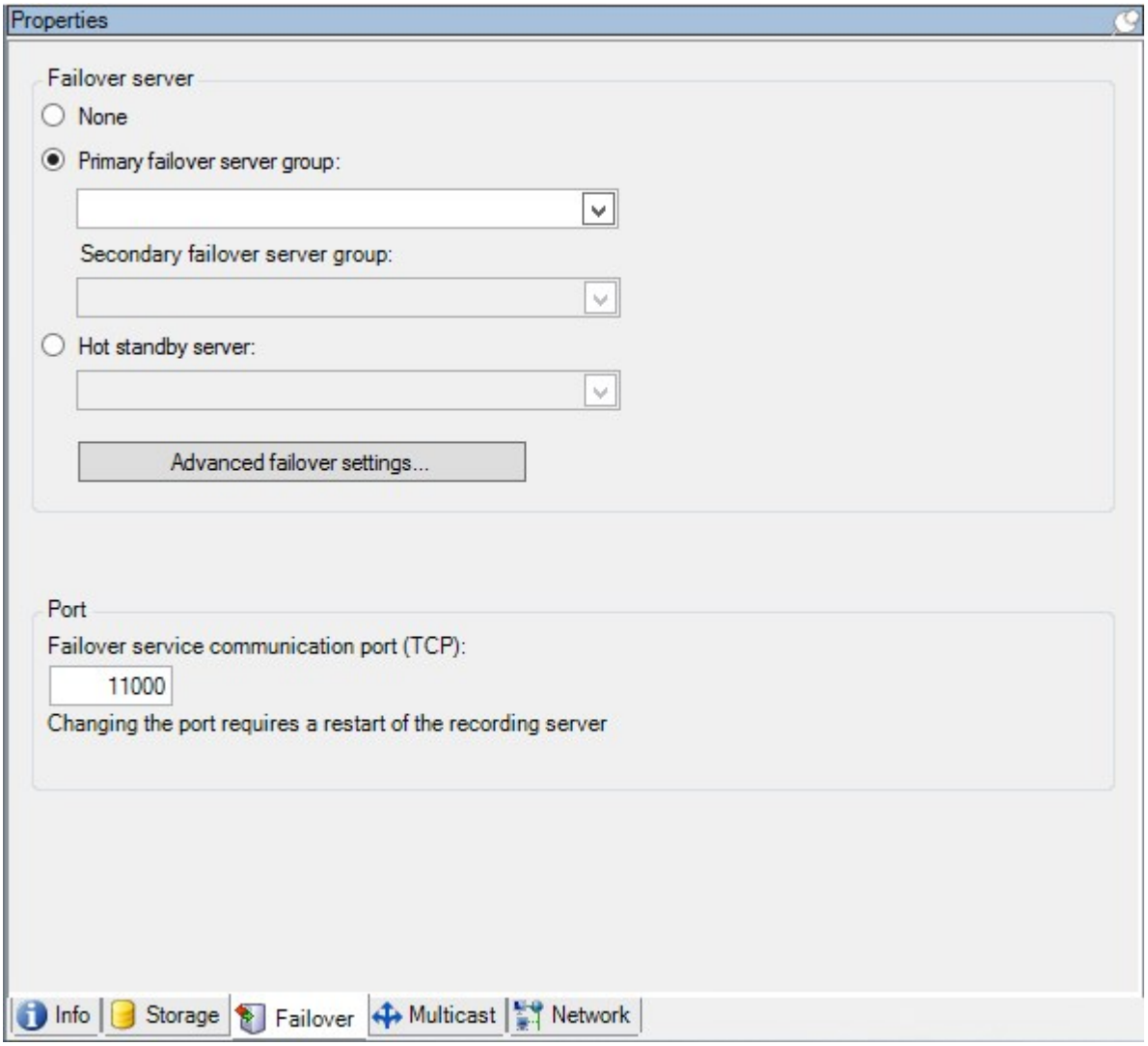
Nombre	Descripción
	Si el directorio no existe, puede crearlo. Las unidades de red deben especificarse utilizando el formato UNC (Convención de Nomenclatura Universal, Universal Naming Convention), por ejemplo: `\\servidor\volumen\directorio\`.
Periodo de retención	Especifique durante cuánto tiempo deben permanecer las grabaciones en el archivo antes de que se eliminen o se muevan al siguiente archivo (dependiendo de los ajustes de archivo). El tiempo de retención siempre debe ser superior al tiempo de retención del archivo previo o la base de datos de grabación predeterminada. Esto se debe a que el número de días de retención especificado para un archivo incluye todos los periodos de retención indicados previamente en el proceso.
Tamaño máximo	Seleccione el número máximo de gigabytes de datos de grabación para guardar en la base de datos de grabaciones. La grabación de datos que supere el número especificado de gigabytes se mueve automáticamente al primer archivo de la lista - si se especifica alguno - o se elimina. ⚠ Cuando hay menos de 5 GB de espacio libre, el sistema siempre autoarchiva (o elimina si no se ha definido ningún próximo archivo) los datos más antiguos en una base de datos. Si hay menos de 1 GB de espacio libre, los datos se eliminan. Una base de datos siempre requiere 250 MB de espacio libre. Si alcanza este límite (si no se eliminan datos lo bastante rápido), no se escriben más datos en la base de datos hasta que haga liberado suficiente espacio. El tamaño máximo real de su base de datos es la cantidad de gigabytes que especifique, menos 5 GB.
Calendario	Especifique un calendario de archivado que describa los intervalos en los que se debe iniciar el proceso de archviado. Puede archiva con mucha frecuencia (en principio cada hora durante todo el año), o con muy poca frecuencia (por ejemplo, cada primer lunes o cada 36 meses).
Reducir velocidad de fotogramas	Para reducir los FPS al archivar, seleccione la casilla de verificación **Reducir velocidad de fotogramas** y establezca un valor de fotogramas por segundo (FPS). La reducción de la velocidad de fotogramas en un número seleccionado de FPS hace que las grabaciones ocupen menos espacio en el archivo, pero también reduce la

Nombre	Descripción
	calidad de su archivo. MPEG-4/H.264/H.265 se reduce automáticamente a fotogramas clave como mínimo. 0,1 = 1 fotograma por 10 segundos.

Pestaña Failover (servidor de grabación)

La funcionalidad disponible depende del sistema que esté utilizando. Vea la lista completa de características, que está disponible en la página de descripción del producto en el sitio web Milestone (https://www.milestonesys.com/solutions/platform/product-index/).

Si su organización utiliza servidores de grabación de failover, utilice la pestaña para asignar servidores de failover a los servidores de grabación; consulte las Propiedades de la pestaña Failover.



Para obtener detalles sobre los servidores de grabación de failover, la instalación y la configuración, los grupos de failover y su configuración, consulte Servidor de grabación de failover (explicación) en la página 37.

Propiedades de la pestaña Failover

Nombre	Descripción
Ninguno	Seleccione una configuración sin servidores de grabación de failover.
Grupo del servidor	Seleccione una configuración de failover regular con un grupo de servidor de

Nombre	Descripción
de failover principal/Grupo del servidor de failover secundario	failover principal y posiblemente uno secundario.
Servidor de espera en caliente	Seleccione una configuración de espera activa con un servidor de grabación dedicado como servidor de espera activa.
Ajustes avanzados de failover	Abre la ventana **Ajustes avanzados de failover**: • **Soporte total**: Habilita el soporte de failover completo para el dispositivo • **Solo directo**: Habilita solo el soporte de failover para cinco flujos en el dispositivo • **Deshabilitado**: Deshabilita el soporte de failover para el dispositivo
Puerto de comunicaciones de servicio de failover (TCP)	De forma predeterminada, el número de puerto es 11000. Utiliza este puerto para la comunicación entre servidores de grabación y servidores de grabación de failover. Si cambia el puerto, el servidor de grabación **debe** estar en ejecución y **debe** estar conectado al servidor de gestión.

Pestaña Multidifusión (servidor de grabación)

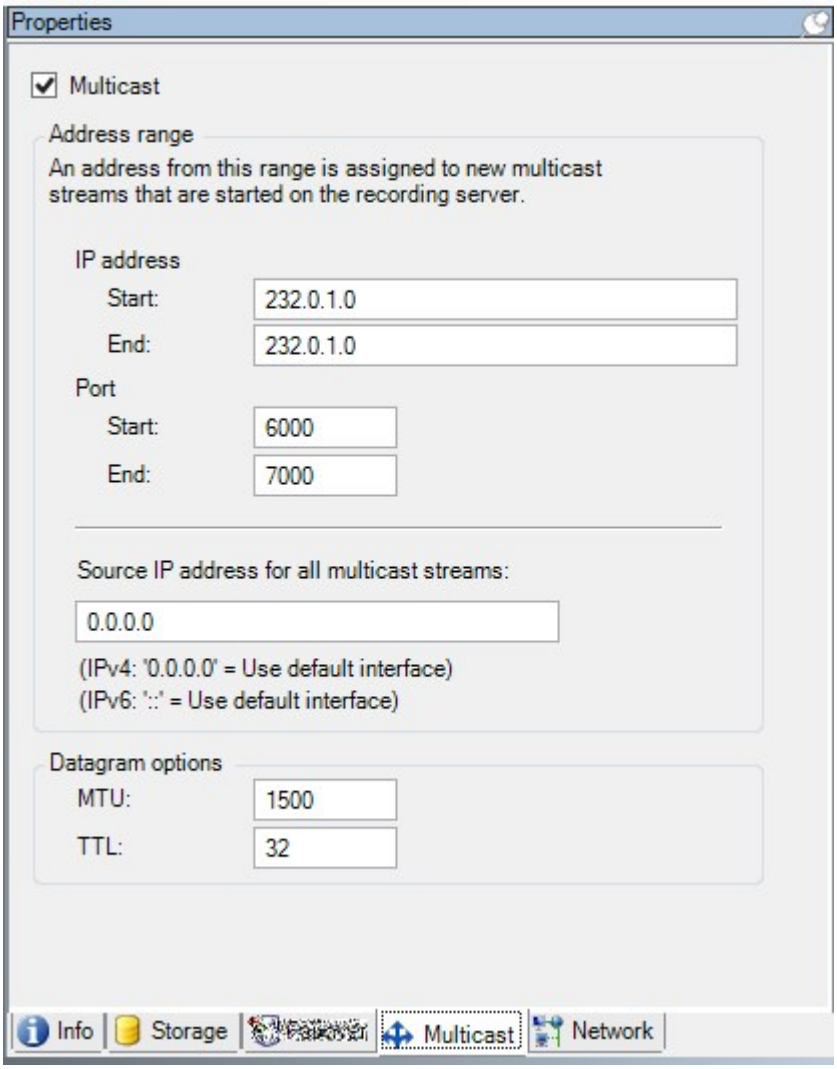
Su sistema admite la multidifusión de flujos en directo desde los servidores de grabación. Si varios usuarios de XProtect Smart Client desean visualizar vídeo en directo desde la misma cámara, la multidifusión ayuda a ahorrar una cantidad considerable de recursos del sistema. La emisión múltiple es particularmente útil si tiene funcionalidad Matrix donde varios clientes precisan vídeo en directo desde la misma cámara.

La retransmisión múltiple solo es posible para flujos en directo, no para vídeo/audio grabado.

Si un servidor de grabación tiene más de una tarjeta de interfaz de red, solo es posible utilizar la multidifusión en una de ellas. A través de Management Client puede especificar cuál usar.

Si utiliza servidores de failover, recuerde especificar también la dirección IP de la tarjeta de interfaz de red en los servidores de failover (consulte Pestaña multidifusión (servidor de failover) en la página 445).

La implementación exitosa de la multidifusión también requiere que haya configurado su equipo de red para retransmitir los paquetes de datos de multidifusión solo al grupo de destinatarios requerido. Si no es así, la multidifusión puede no ser diferente de la difusión, lo que puede ralentizar considerablemente la comunicación de la red.



Asignar rango de direcciones IP

Especifique el rango que quiere asignar como direcciones para flujos multidifusión para el servidor de grabación seleccionado. Los clientes se conectan a estas direcciones cuando los usuarios ven vídeo multidifusión desde el servidor de grabación.

Para cada contenido de cámara de multidifusión, la combinación de dirección IP y puerto debe ser única (ejemplo de IPv4: 232.0.1.0:6000). Puede usar una dirección IP y muchos puertos o muchas direcciones IP y pocos puertos. De forma predeterminada, el sistema sugiere una única dirección IP y un rango de 1000 puertos, pero puede cambiar esto según sea necesario.

Las direcciones IP para multidifusión deben estar dentro del rango definido para asignación de host dinámico mediante IANA. IANA el la autoridad que supervisa la asignación de direcciones IP globales.

Nombre	Descripción
Dirección IP	En el campo **Iniciar**, especifique la primera dirección IP en el rango requerido. A continuación, especifique la última dirección IP en el rango 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 todos los flujos multidifusión	Solo puede realizar multidifusión en una tarjeta de interfaz de red, de modo que este campo es relevante si su servidor de grabación 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 predeterminada del servidor de grabación, deje el valor 0.0.0.0 (IPv4) o: (IPv6) en el campo. Si quiere utilizar otra tarjeta de interfaz de red o una dirección IP distinta 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, el rango se describe en el sitio web de IANA (https://www.iana.org/).

Especificar opciones de datagramas

Especifique los justes para paquetes de datos (datagramas) transmitidos mediante multidifusión.

Nombre	Descripción
MTU	Unidad de transmisión máxima, el tamaño del paquete de datos físico más grande permitido (medido en bytes). Los mensajes mayores a la MTU especificada se dividen en paquetes más pequeños antes de su envío. El valor predeterminado es 1500, que también

Nombre	Descripción
	es el valor predeterminado en la mayoría de ordenadores Windows y redes Ethernet.
TTL	Tiempo hasta Directo, la mayor cantidad permitida de saltos que un paquete de datos debería poder viajar antes de ser descartado o devuelto. Un salto es un punto entre dos dispositivos de red, normalmente un router. El valor predeterminado es 128.

Pestaña Red (servidor de grabación)

Si necesita acceder al VMS con XProtect Smart Client a través de una red pública o no fiable, Milestone le recomienda que utilice una conexión segura a través de VPN. Esto ayuda a garantizar que la comunicación entre XProtect Smart Client y el servidor VMS está protegida.

Define una dirección IP pública del servidor de grabación en la pestaña **Red**.

¿Por qué utilizar una dirección pública?

Los clientes pueden conectarse tanto desde la red local como desde Internet, y en ambos casos el sistema de vigilancia debe proporcionar las direcciones adecuadas para que los clientes puedan acceder al vídeo en directo y al grabado desde los servidores de grabación:

- Cuando los clientes se conectan localmente, el sistema de vigilancia debe responder con direcciones y números de puerto locales
- Cuando los clientes se conectan desde Internet, el sistema de vigilancia debe responder con la dirección pública del servidor de grabación. Es la dirección del cortafuegos o del router NAT (Network Address Translation), y a menudo también un número de puerto diferente. La dirección y el puerto pueden entonces ser reenviados a la dirección y el puerto locales del servidor.

Servidores de failover (nodo Servidores)

La funcionalidad disponible depende del sistema que esté utilizando. Vea la lista completa de características, que está disponible en la página de descripción del producto en el sitio web Milestone (https://www.milestonesys.com/solutions/platform/product-index/).

Un servidor de grabación de failover es un servidor de grabación adicional que sustituye al servidor de grabación estándar si éste no está disponible. Puede configurar un servidor de grabación de failover en dos modos, como **servidor de espera en frío** o como **servidor de espera en caliente**.

Los servidores de grabación failover se instalan como los servidores de grabación estándar (consulte Instalar un servidor de grabación de failover a través de Download Manager en la página 175). Una vez que haya instalado los servidores de grabación de failover, serán visibles en el Management Client. Milestone recomienda que instale todos los servidores de grabación de failover en ordenadores separados. Asegúrese de configurar los servidores de grabación de failover con la dirección IP/nombre de host correctos del servidor de gestión. Los permisos de usuario para la cuenta de usuario bajo la que se ejecuta el servicio del servidor de failover se proporcionan durante el proceso de instalación. Estos son:

- Permisos de inicio/detención para iniciar o detener el servidor de grabación de failover
- Permisos de acceso de lectura y escritura para leer o escribir el archivo RecorderConfig.xml

Si se selecciona un certificado para el cifrado, el administrador debe conceder permiso de acceso de lectura al usuario de failover sobre la clave privada del certificado seleccionado.

Si el servidor de grabación de failover se hace cargo de un servidor de grabación que utiliza cifrado, Milestone recomienda preparar también el servidor de grabación de failover para que utilice el cifrado. Si desea más información, consulte Comunicación segura (explicación) en la página 150 y Instalar un servidor de grabación de failover a través de Download Manager en la página 175.

Puede especificar qué tipo de soporte de failover desea a nivel de dispositivo. Para cada dispositivo de un servidor de grabación, seleccione soporte completo, solo en directo o sin failover. Esto le ayuda a priorizar sus recursos de failover y, por ejemplo, a configurar solo el failover para el vídeo y no para el audio, o solo tener failover en las cámaras esenciales y no en las menos importantes.

Mientras el sistema está en modo de failover, no se puede reemplazar o mover el hardware, actualizar el servidor de grabación o cambiar las configuraciones de los dispositivos, como los ajustes de almacenamiento o de flujo de vídeo.

Servidores de grabación de failover en frío

En una configuración de servidor de grabación de failover en frío, se agrupan varios servidores de grabación de failover en un grupo de failover. Todo el grupo de failover está dedicado a hacerse cargo de cualquiera de los varios servidores de grabación preseleccionados, si uno de ellos deja de estar disponible. Puede crear tantos grupos como desee (consulte Servidores de grabación de failover en grupo para la espera en frío en la página 215).

La agrupación tiene una clara ventaja: cuando se especifica posteriormente qué servidores de grabación de failover deben tomar el relevo de un servidor de grabación, se selecciona un grupo de servidores de grabación de failover. Si el grupo seleccionado contiene más de un servidor de grabación de failover, este le ofrece la

seguridad de tener más de un servidor de grabación de failover listo para tomar el relevo si un servidor de grabación no está disponible. Puede especificar un grupo de servidores de failover secundario que tome el relevo del grupo primario si todos los servidores de grabación del grupo primario están ocupados. Un servidor de grabación de failover solo puede ser miembro de un grupo a la vez.

Los servidores de grabación de failover en un grupo de failover se ordenan en una secuencia. La secuencia determina el orden en el que los servidores de grabación de failover se harán cargo de un servidor de grabación. Por defecto, la secuencia refleja el orden en el que ha incorporado los servidores de registro de failover en el grupo de failover: el primero en es el primero en la secuencia. Puede cambiarlo si lo necesita.

Servidores de grabación por failover en caliente

En una configuración de servidor de grabación de failover en caliente, se dedica un servidor de grabación de failover para encargarse solo de **un** servidor de grabación. Debido a esto, el sistema puede mantener este servidor de grabación de failover en 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 el relevo mucho más rápido que un servidor de grabación de failover en espera fría. Como se ha mencionado, asigna servidores de espera en caliente a un solo servidor de grabación y no se pueden agrupar. No puede asignar servidores de failover que ya formen parte de un grupo de failover como servidores de grabación de espera en caliente.

Validación del servidor de grabación de failover

Para validar una fusión de datos de vídeo desde el servidor de failover al servidor de grabación, debe hacer que el servidor de grabación no esté disponible deteniendo el servicio del servidor de grabación o apagando el ordenador del servidor de grabación.

Cualquier interrupción manual de la red que pueda provocar tirando del cable de red o bloqueando la red con una herramienta de prueba no es un método válido.

Propiedades de la pestaña Información (servidor de failover)

Especifique las siguientes propiedades del servidor de grabación de failover:

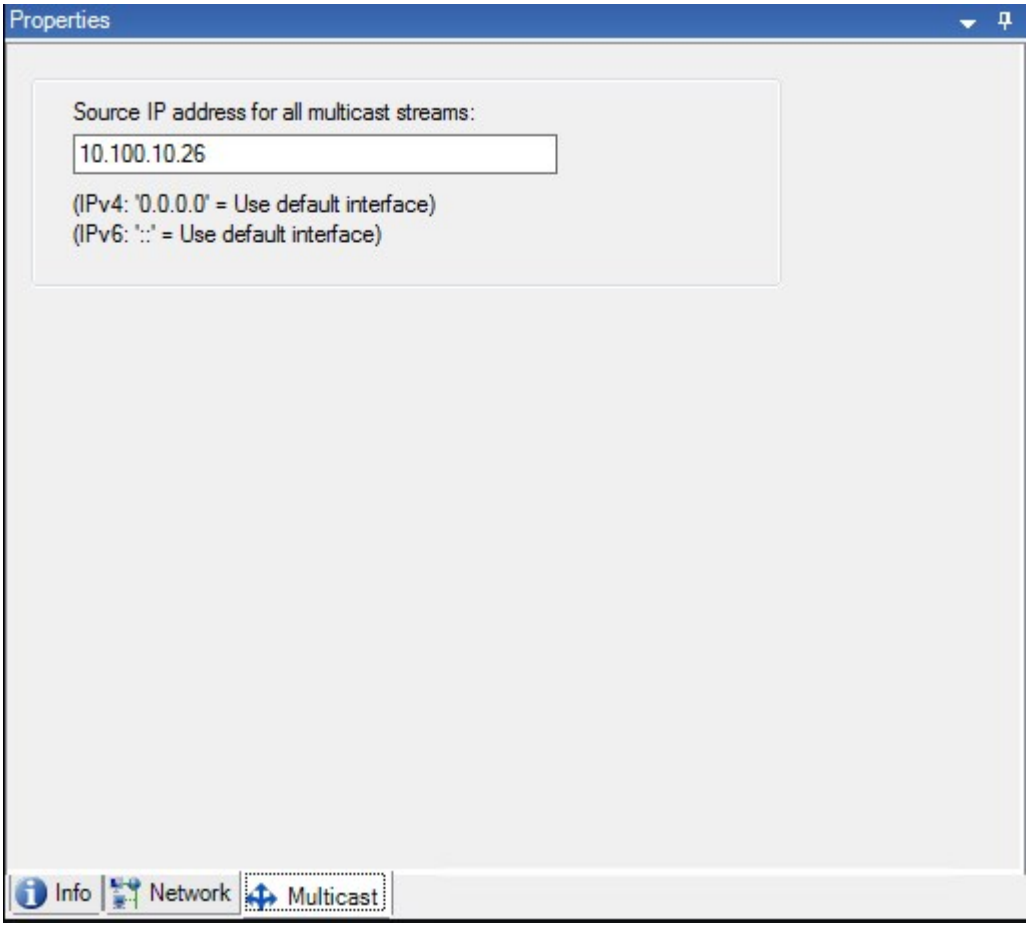
Nombre	Descripción
Nombre	El nombre del servidor de grabación de failover tal como aparece en Management

Nombre	Descripción
	Client, en los registros y más.
Descripción	Un campo opcional que puede usar para describir el servidor de grabación de failover, por ejemplo que de qué servidor de grabación asume el control.
Nombre de host	Muestra el nombre del host del servidor de grabación de failover. No puede cambiar esto.
Dirección del servidor web local	Muestra la dirección local del servidor web del servidor de grabación de failover. Usted utiliza la dirección local, por ejemplo, para gestionar comandos de control de cámaras PTZ, y para gestionar la navegación y las solicitudes en directo desde XProtect Smart Client. La dirección incluye el número de puerto que se usa para la comunicación con el servidor web (normalmente puerto 7563). Si el servidor de grabación de failover asume el control desde un servidor de grabaciones que utiliza encriptación, también debe preparar el servidor de grabaciones de failover para usar encriptación. Si habilita la encriptación a clientes y servidores que recuperan flujos de datos del servidor de grabación, aparece el icono de un candado, y la dirección incluye **https** en lugar de **http**.
Dirección de servidor web	Muestra la dirección pública del servidor web del servidor de grabación de failover en Internet. Si su instalación utiliza un cortafuegos o enrutador NAT, introduzca la dirección del cortafuegos o del enrutador NAT para que los clientes que acceden al sistema de vigilancia en Internet puedan conectarse al servidor de grabación de failover. Usted especifica la dirección pública y el número de puerto en la pestaña **Red**. Si habilita la encriptación a clientes y servidores que recuperan flujos de datos del servidor de grabación, aparece el icono de un candado, y la dirección incluye **https** en lugar de **http**.
Puerto UDP	El número de puerto utilizado para la comunicación entre servidores de grabación de failover. El puerto predeterminado es 8844.

Nombre	Descripción
Ubicación de la base de datos	Especifique la ruta de la base de datos utilizada por el servidor de grabación de failover para almacenar grabaciones. No puede cambiar la ruta de la base de datos mientras el servidor de grabación de failover está asumiendo el control desde un servidor de grabación. El sistema aplica los cambios cuando el servidor de grabación de failover ha dejado de asumir el control desde un servidor de grabación.
Habilitar este servidor failover	Desactivar para deshabilitar el servidor de grabación de failover (seleccionado de forma predeterminada). Debe deshabilitar servidores de grabación de failover antes de poder asumir el control de servidores de grabación.

Pestaña multidifusión (servidor de failover)

Si está utilizando servidores de failover y ha habilitado la multidifusión de transmisión en directo, 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 failover.



Para obtener información adicional sobre multidifusión, consulte Habilitar la multidifusión para el servidor de grabación en la página 210.

Propiedades de la pestaña Información (grupo de failover)

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

Propiedades de la pestaña Secuencia (grupo de failover)

Campo	Descripción
Especificar la secuencia de failover	Utilice **Arriba** y **Abajo** para establecer la secuencia deseada de servidores normales de grabación de failover dentro del grupo.

Servidor remoto para Milestone Interconnect

Milestone Interconnect™ le permite integrar una serie de instalaciones más pequeñas, físicamente fragmentadas e instalaciones remotas XProtect con un sitio central XProtect Corporate. Puede instalar estos sitios más pequeños, llamados sitios remotos, en unidades móviles, por ejemplo, barcos, autobuses o trenes. Esto significa que estos sitios no necesitan estar permanentemente conectados a una red.

Pestaña Información (servidor remoto)

Nombre	Descripción
Nombre	El sistema utiliza el nombre siempre que el servidor remoto esté recogido en el sistema y en los clientes. No es necesario que el nombre sea único. Cuando cambia el nombre de un servidor, el nombre se cambia globalmente en el Management Client.
Descripción	Introduzca una descripción del servidor remoto (opcional). La descripción aparece en varios listados del sistema. Por ejemplo, al pausar el puntero del ratón sobre el nombre del hardware en el panel **Descripción general**.
Modelo	Muestra el producto de 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.

Nombre	Descripción
Controlador	Identifica el controlador que maneja la conexión con el servidor remoto.
Dirección	El nombre del host o la dirección IP del hardware.
IE	Abre la página de inicio predeterminada del proveedor de hardware. Puede utilizar esta página para la administración del hardware o del sistema.
ID del sistema remoto	El ID único del sistema del sitio remoto utilizado por XProtect para, por ejemplo, gestionar licencias.

Pestaña Ajustes (servidor remoto)

En la pestaña **Ajustes**, puede ver el nombre del sistema remoto.

Pestaña Eventos (servidor remoto)

Puede añadir eventos del sistema remoto a su sitio central con el fin de crear reglas y, de este modo, responder inmediatamente a eventos del sistema remoto. El número de eventos depende de los eventos configurados en el sistema remoto. No puede eliminar eventos predeterminados.

Si la lista parece estar incompleta:

1. Haga clic con el botón derecho en el servidor remoto relevante en el panel **Descripción general** y seleccione **Actualizar hardware**.
2. El cuadro de diálogo recoge todos los cambios (dispositivos quitados, actualizados y añadidos) en el sistema remoto desde que estableció o actualizó por última vez la configuración de Milestone Interconnect. Haga clic en **Confirmar** para actualizar su sitio central con estos cambios.

Pestaña Recuperación remota

En la pestaña **Recuperación remota**, puede manejar ajustes de recuperación de grabaciones remotas para el sitio remoto en una configuración de Milestone Interconnect:

Especifique las siguientes propiedades:

Nombre	Descripción
Recuperar grabaciones al máximo	Determina el ancho de banda máximo en Kbits/s que se va a usar para recuperar grabaciones desde un sitio remoto. Seleccione la casilla de verificación para habilitar la limitación de recuperaciones.
Recuperar grabaciones entre	Determina que la recuperación de grabaciones desde un sitio remoto está limitada a un intervalo de tiempo concreto. Los trabajos sin terminar en la hora de finalización continúan hasta que terminan, de modo que, si la hora de finalización es crítica, debe definirla antes para permitir que los trabajos sin terminar se completen. Si el sistema recibe una recuperación automática o una solicitud de recuperación del XProtect Smart Client fuera del intervalo de timempo, se acepta, pero no comienza hasta que se ha alcanzado el intervalo de tiempo seleccionado. Puede ver trabajos de recuperación de grabaciones remotas pendientes iniciados por los usuarios desde **Panel del sistema** -> **Tareas actuales**.
Recuperar en dispositivos en paralelo	Determina el número máximo de dispositivos desde lo que se recuperan grabaciones de forma simultánea. Cambie el valor predeterminado si necesita más o menos capacidad dependiendo de las capacidades de su sistema.

Cuando cambie los ajustes, pueden pasar varios minutos hasta que los cambios se vean reflejados en el sistema.

Ninguno de los anteriores se aplica a la reproducción directa de grabaciones remotas. Todas las cámaras establecidas para ser reproducidas directamente están disponibles para la reproducción directa y para usar ancho de banda según sea necesario.

Nodo de dispositivos

Dispositivos (nodo Dispositivos)

Los dispositivos aparecen en Management Client cuando añade hardware con el asistente **Añadir hardware**. Consulte Añadir hardware en la página 217.

Puede gestionar dispositivos mediante los grupos de dispositivos si tienen las mismas propiedades, consulte Device groups (explicación) en la página 55.

También puede gestionar los dispositivos individualmente.

La deshabilitación/deshabilitación y el cambio de nombre de dispositivos individuales se produce en el hardware del servidor de grabación. Consulte Habilitar(Deshabilitar dispositivos mediante grupos de dispositivos.

Para el resto de la configuración y la gestión de cámaras, expanda **Dispositivos** en el panel Navegación en el sitio y, a continuación, seleccione un dispositivo:

- **Cámaras**
- **Micrófonos**
- **Altavoces**
- **Metadatos**
- **Entradas**
- **Salidas**

En el panel Descripción general, agrupe sus cámaras para una descripción general fácil de sus cámaras. El agrupamiento inicial se hace como parte del asistente **Añadir hardware**.

Para obtener información sobre el hardware compatible, consulte la página de hardware compatible en el sitio web Milestone (https://www.milestonesys.com/support/tools-and-references/supported-devices/).

Iconos de estado de dispositivos

Al seleccionar un dispositivo, la información sobre el estado actual aparece en el panel **Vista previa**.
Los siguientes iconos indican el estado de los dispositivos:

Cámara	Micrófono	Altavoz	Metadatos	Entrada	Salida	Descripción
						**Dispositivo habilitado y recuperando datos**: El dispositivo está habilitado y usted recupera una transmisión en directo.

Cámara	Micrófono	Altavoz	Metadatos	Entrada	Salida	Descripción
						**Dispositivo grabando**: El dispositivo está grabando datos en el sistema.
						**Dispositivo temporalmente detenido o no recibe contenido**: Cuando se para, no se transfiere información al sistema. Si es una cámara, no puede ver vídeo en directo. Un dispositivo parado aún puede comunicarse con el servidor de grabación para recuperar eventos, ajustar configuraciones, etc, en oposición a cuando se deshabilita un dispositivo.
						**Dispositivos deshabilitados**: No se puede iniciar automáticamente por medio de una regla y no se puede comunicar con el servidor de grabaciones. Si

Cámara	Micrófono	Altavoz	Metadatos	Entrada	Salida	Descripción
						una cámara está deshabilitada, no puede ver vídeo en directo ni grabado.
						**La base de datos de dispositivos se está reparando**.
						**El dispositivo requiere atención**: El dispositivo no funciona correctamente. Pause el puntero del ratón sobre el icono del dispositivo para obtener una descripción del problema en la información sobre herramientas.
						**Estado desconocido**: El estado del dispositivo se desconoce, por ejemplo, si el servidor de grabaciones está fuera de línea.
						Algunos iconos se pueden combinar, como en este ejemplo en el que

Cámara	Micrófono	Altavoz	Metadatos	Entrada	Salida	Descripción
						Dispositivo habilitado y recuperando datos se combina con **Dispositivo grabando**.

Cámaras (nodo Dispositivos)

Los dispositivos de cámara se añaden automáticamente al añadir hardware al sistema y, de forma predeterminada, están habilitados.

El sistema incluye una regla de inicio de alimentación de contenido predeterminada que garantiza que los contenidos de vídeo desde todas las cámaras conectadas se alimenten automáticamente al sistema. La regla predeterminada se puede desactivar y/o modificar según las necesidades.

Siga este orden de configuración para completar las tareas más típicas relacionadas con la configuración en un dispositivo de cámara:

1. Configure los ajustes de la cámara, consulte pestaña Ajustes (dispositivos.
2. Configure flujos, consulte pestaña Flujos (dispositivos).
3. Configure el movimiento, consulte pestaña Movimiento (dispositivos).
4. Configure la grabación, consulte pestaña Grabar (dispositivos) y Monitorizar las bases de datos para dispositivos.
5. Configure el resto de ajustes según sea necesario.

Micrófonos (nodo DIspositivos)

Los dispositivos de micrófonos se añaden automáticamente al añadir hardware al sistema. De forma predeterminada, están deshabilitados, por lo que debe habilitarlos antes de usarlos, ya sea como parte del asistente **Añadir Hardware** o posteriormente. Los micrófonos no requieren licencias separadas. Puede utilizar tantos micrófonos como necesite en su sistema.

Puede utilizar micrófonos de forma totalmente independiente de las cámaras.

El sistema incluye una regla de fuente de audio de inicio predeterminada que garantiza que los contenidos de audio de todos los micrófonos conectados se alimenten automáticamente al sistema. La regla predeterminada se puede desactivar y/o modificar según las necesidades.

Puede configurar dispositivos de micrófonos en estas pestañas:

- Pestaña Información, consulte Pestaña Información (dispositivos)
- Pestaña Ajustes, consultar Pestaña Ajustes (dispositivos)
- Pestaña Grabar, consultar Pestaña Grabar (dispositivos)
- Pestaña Eventos, consulte Pestaña eventos (dispositivos)

Altavoces (nodo Dispositivos)

Los dispositivos altavoces se añaden automáticamente al añadir hardware al sistema. De forma predeterminada, están deshabilitados, por lo que debe habilitarlos antes de usarlos, ya sea como parte del asistente **Añadir Hardware** o posteriormente. Los altavoces no requieren licencias separadas. Puede utilizar tantos altavoces como sea necesario en su sistema.

Puede usar altavoces de manera completamente independiente de las cámaras.

El sistema incluye una regla de inicio de contenido de audio predeterminada que inicia el dispositivo de modo que este esté listo para enviar al usuario activado audio a los altavoces. La regla predeterminada se puede desactivar y/o modificar según las necesidades.

Puede configurar dispositivos de altavoz en estas pestañas:

- Pestaña Información, consulte Pestaña Información (dispositivos)
- Pestaña Ajustes, consultar Pestaña Ajustes (dispositivos)
- Pestaña Grabar, consultar Pestaña Grabar (dispositivos)

Metadatos (nodo Dispositivos)

El sistema incluye una regla de inicio de alimentación de contenido predeterminada que garantiza que los contenidos de metadatos desde todo el hardware conectado que admite metadatos se alimenten automáticamente al sistema. La regla predeterminada puede desactivarse y/o modificarse según las necesidades.

Puede configurar dispositivos de metadatos en estas pestañas:

- Pestaña Información, consulte Pestaña Información (dispositivos)
- Pestaña Ajustes, consultar Pestaña Ajustes (dispositivos)
- Pestaña Grabar, consultar Pestaba Grabar (dispositivos)

Entrada (nodo Dispositivos)

Puede utilizar dispositivos de entrada de forma totalmente independiente de las cámaras.

> Antes de especificar el uso de unidades de entrada externas, verifique que el propio dispositivo reconoce el funcionamiento del sensor. La mayoría de los dispositivos pueden mostrar esto en sus interfaces de configuración o mediante comandos de la secuencia de comandos de Common Gateway Interface (CGI).

Los dispositivos de entrada se añaden automáticamente al añadir hardware al sistema. De forma predeterminada, están deshabilitados, por lo que debe habilitarlos antes de usarlos, ya sea como parte del asistente **Añadir Hardware** o posteriormente. Los dispositivos de entrada no requieren licencias separadas. Puede utilizar tantos dispositivos de entrada como necesite en su sistema.

Puede configurar dispositivos de entrada en estas pestañas:

- Pestaña Información, consulte Pestaña Información (dispositivos)
- Pestaña Ajustes, consultar Pestaña Ajustes (dispositivos)
- Pestaña Eventos, consulte Pestaña eventos (dispositivos)

Salida (nodo Dispositivos)

La salida puede desencadenarse manualmente desde Management Client y XProtect Smart Client.

> Antes de especificar el uso de unidades de entrada externas en un dispositivo, verifique que el propio dispositivo puede controlar el dispositivo conectado a la salida. La mayoría de los dispositivos pueden mostrar esto en sus interfaces de configuración o mediante comandos de la secuencia de comandos de Common Gateway Interface (CGI).

Los dispositivos de salida se añaden automáticamente al añadir hardware al sistema. De forma predeterminada, están deshabilitados, por lo que debe habilitarlos antes de usarlos, ya sea como parte del asistente **Añadir Hardware** o posteriormente. Los dispositivos de salida no requieren licencias separadas. Puede utilizar tantos dispositivos de salida como necesite en su sistema.

Puede configurar dispositivos de salida en estas pestañas:

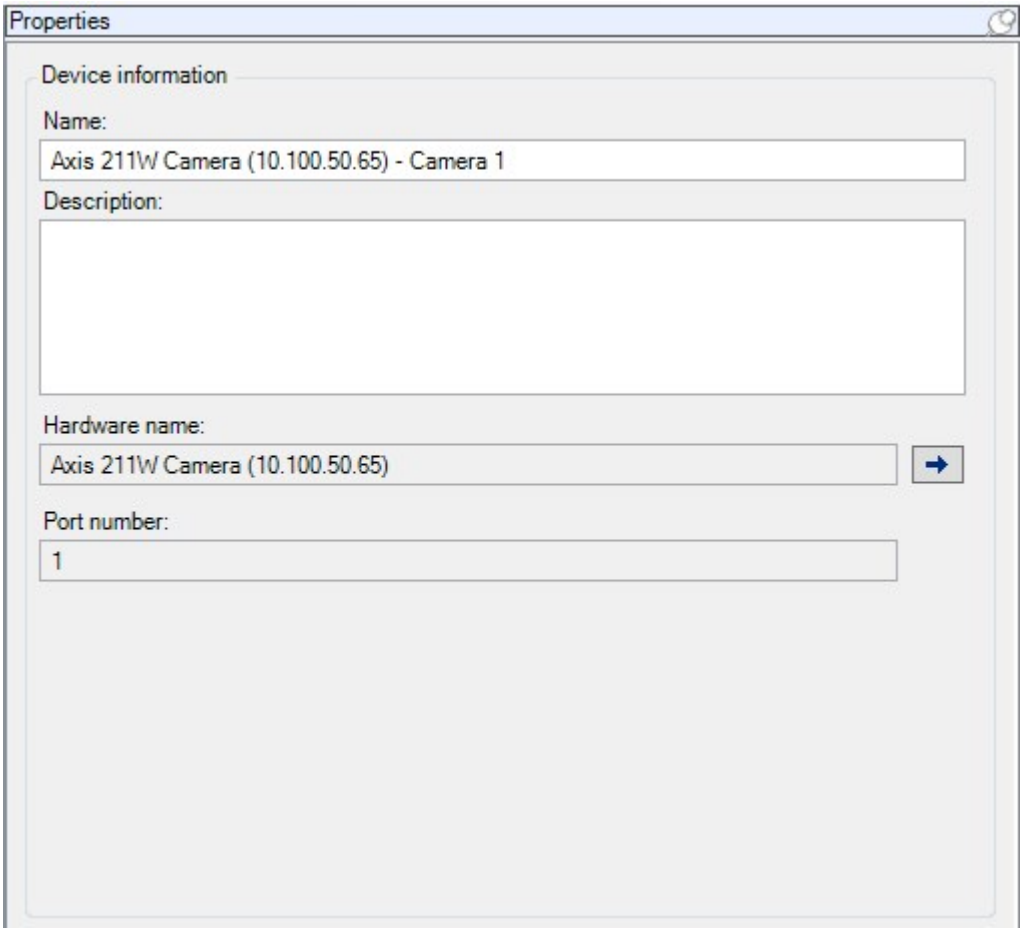
Pestaña Información, ver

- Pestaña Información, consulte Pestaña Información (dispositivos)
- Pestaña Ajustes, consultar Pestaña Ajustes (dispositivos)

Pestañas de Dispositivos

Pestaña información (dispositivos)

En la pestaña **Información**, puede ver y editar información básica sobre un dispositivo en una serie de campos.
Todos los dispositivos tienen una pestaña **Información**.



Propiedades de la pestaña Información

Nombre	Descripción
Nombre	El nombre se usa cada vez que el dispositivo se enumera en el sistema y en los clientes.

Nombre	Descripción
	Al cambiar el nombre de un dispositivo, el nombre cambia globalmente en Management Client.
Descripción	Introduzca una descripción del dispositivo (opcional). La descripción aparece en varios listados del sistema. Por ejemplo, cuando se pone en pausa el puntero del ratón sobre el nombre en el panel **Descripción general**.
Nombre de hardware	Muestra el nombre del hardware al que el dispositivo está conectado. El campo es no editable desde aquí, pero puede cambiarlo haciendo clic en **Ir a** al lado. Esto le lleva a la información del hardware donde puede cambiar el nombre.
Número de puerto	Muestra el puerto al que está conectado el dispositivo en el hardware. Para hardware de un solo dispositivo, el número de puerto normalmente es **1**. Para hardware de varios dispositivos, como servidores de vídeo con varios canales, el número de puerto normalmente indica el canal al que está conectado el dispositivo, por ejemplo **3**.
Nombre corto	Para aplicar un nombre corto para una cámara, introdúzcalo aquí. La longitud máxima de caracteres es 128. Si está utilizando un plano inteligente, automáticamente se muestra el nombre corto con la cámara en el plano inteligente. De lo contrario, se muestra el nombre completo.
Coordenadas GPS	Introduzca la ubicación geográfica en el formato **latitud, longitud**. El valor que introduzca determina el posición del icono de la cámara en el plano inteligente en XProtect Smart Client. El campo es principalmente para integraciones de terceros e integraciones de planos inteligentes.
Dirección	Introduzca la dirección de visualización de la cámara medida respecto a un punto norte en un eje vertical. El valor que introduzca determina la dirección del icono de la cámara en el plano inteligente en XProtect Smart Client. El valor predeterminado es 0,0.

Nombre	Descripción
	El campo es principalmente para integraciones de terceros e integraciones de planos inteligentes.
Campo de vista	Introduzca el campo de visión en grados. El valor que introduzca determina la vista del icono de la cámara en el plano inteligente en XProtect Smart Client. El valor predeterminado es 0,0. El campo es principalmente para integraciones de terceros e integraciones de planos inteligentes.
Profundidad	Introduzca la profundidad de la cámara en metros o pies. El valor que introduzca 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 integraciones de terceros e integraciones de planos inteligentes.
Obtener vista previa de la posición en el explorador	Para verificar que ha introducido las coordinadas geográficas 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 integraciones de terceros e integraciones de planos inteligentes.

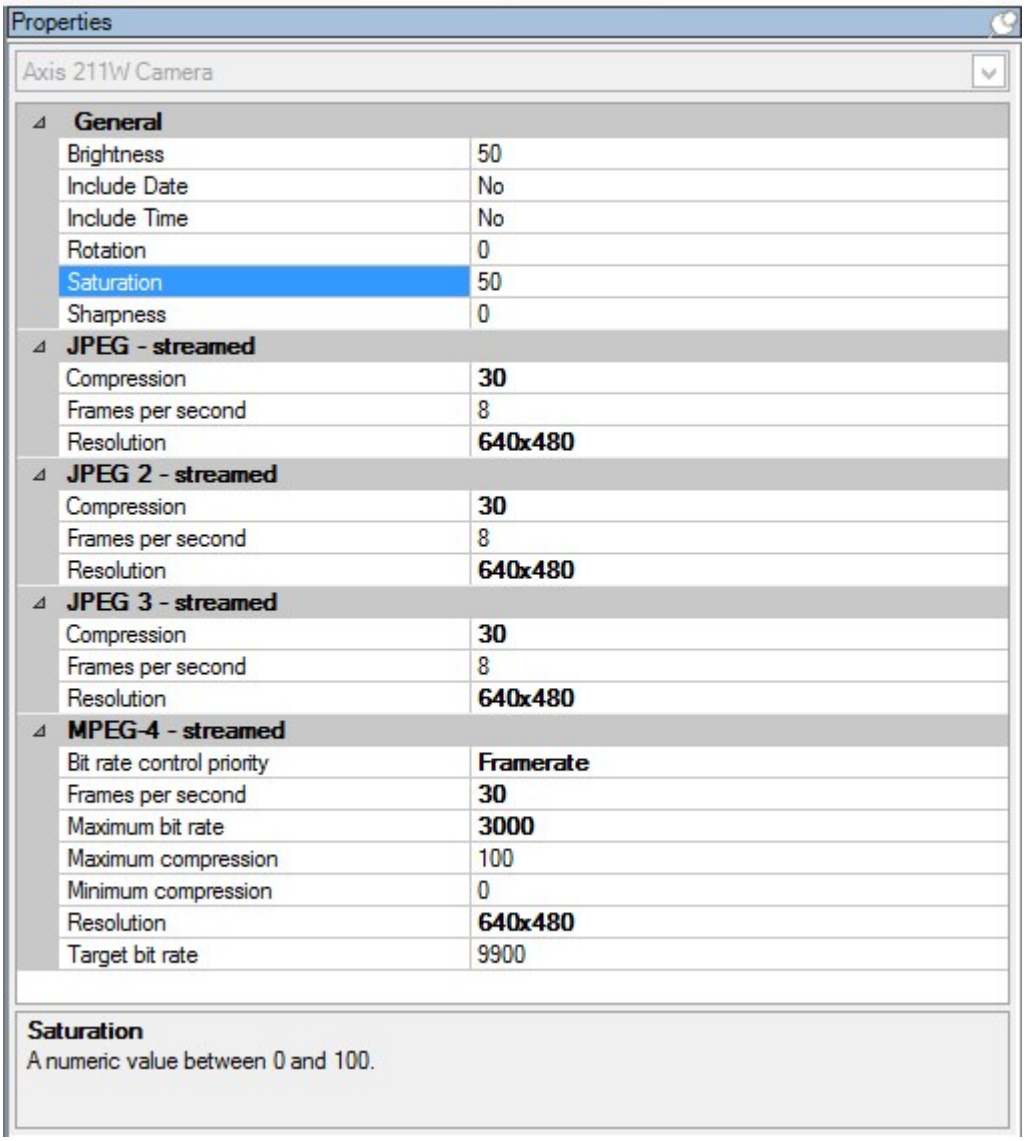
Pestaña Ajustes (dispositivos)

En la pestaña **Ajustes**, puede ver y editar ajustes para un dispositivo en una serie de campos.
Todos los dispositivos tienen una pestaña **Ajustes**.

Los valores aparecen en una tabla como cambiables o de solo lectura. Cuando cambia un ajuste de un valor no predeterminado, el valor aparece en negrita.

El contenido de la tabla depende del controlador del dispositivo.

Los rangos permitidos aparecen en el cuadro de información de debajo de la tabla de ajustes:



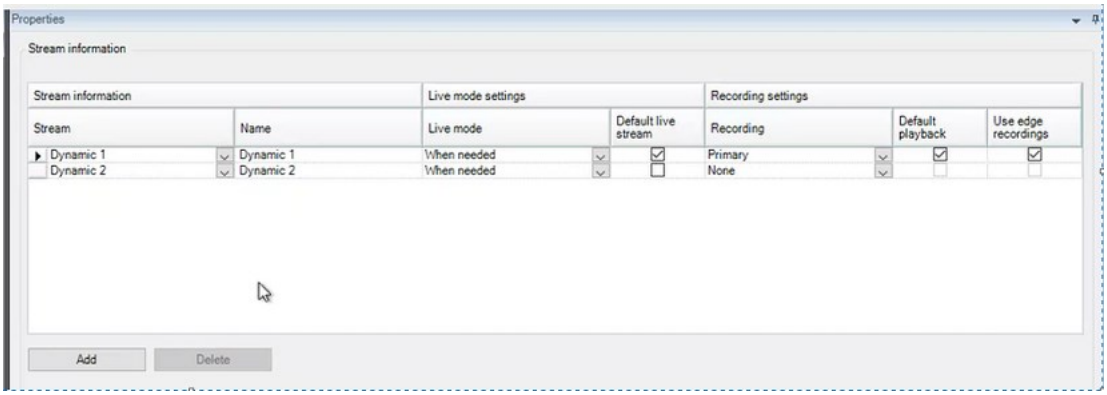
Para obtener información adicional sobre ajustes de la cámara, consulte Ver o editar ajustes de cámara.

Pestaña Flujos (dispositivos)

Los siguientes dispositivos tienen una pestaña **Flujos**:

- Cámaras

La pestaña **Flujos** enumera de forma predeterminada un flujo único. Es el flujo predeterminado de la cámara seleccionada, utilizado para vídeo en directo y grabado. Si utiliza reproducción adaptativa, deberán crearse dos flujos.



Tareas en la pestaña Flujos

Nombre	Descripción
Añadir	Haga clic para añadir un flujo a la lista. Añadir un flujo

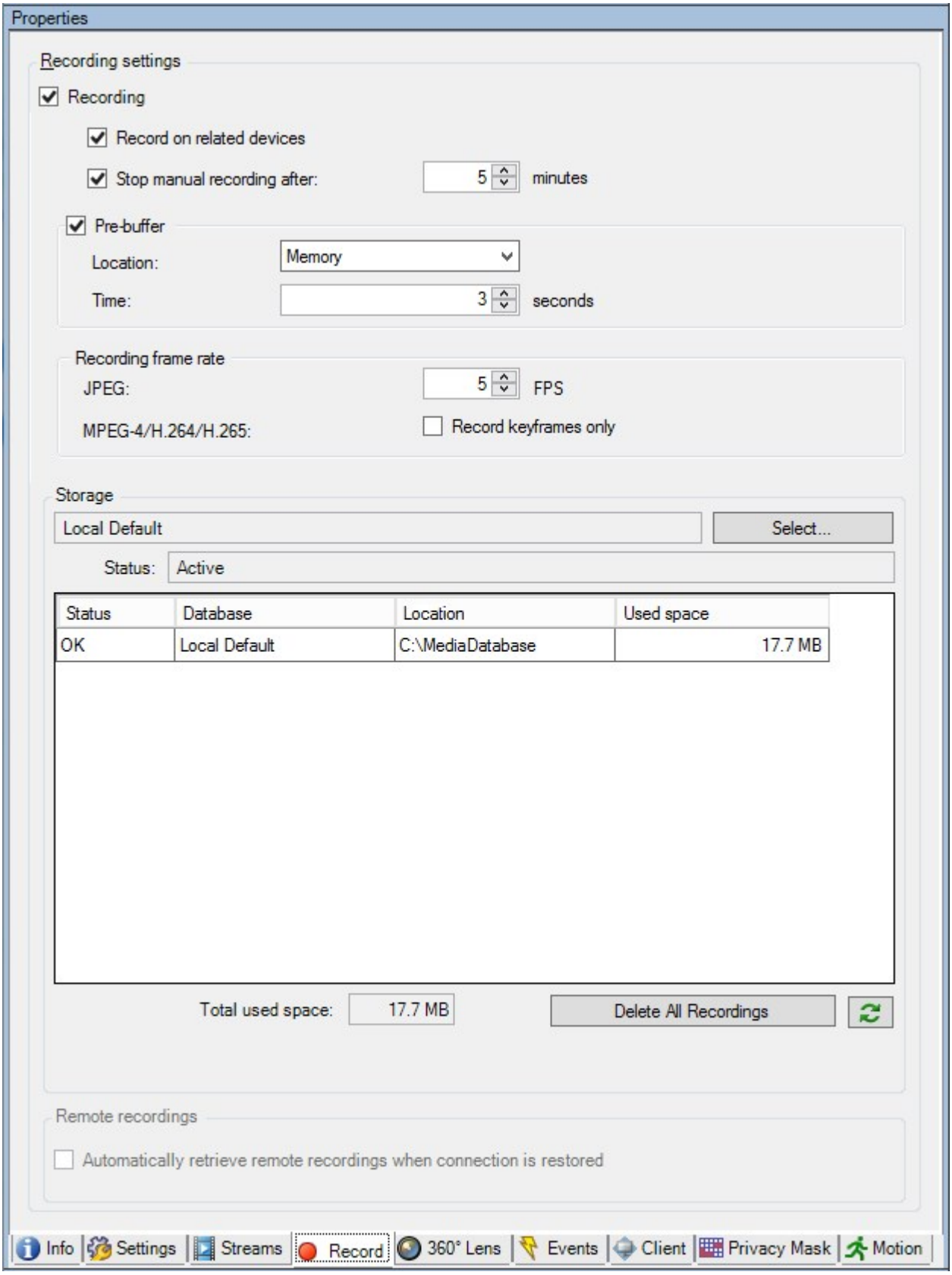
Pestaña Grabar (dispositivos)

Los siguientes dispositivos tienen una pestaña **Grabar**:

- Cámaras
- Micrófonos
- Altavoces
- Metadatos

Las grabaciones desde un dispositivo solo se guardan en la base de datos cuando se ha habilitado la grabación y se cumplen los criterios de las reglas relacionadas con las grabaciones.

Los parámetros que no se pueden configurar para un dispositivo aparecen atenuados.


Properties
Recording settings
Recording
Record on related devices
Stop manual recording after:
5
minutes
Pre-buffer
Location:
Memory
Time:
3
seconds
Recording frame rate
JPEG:
5
FPS
MPEG-4/H.264/H.265:
Record keyframes only
Storage
Local Default
Select...
Status:
Active
Status
Database
Location
Used space
OK
Local Default
C:\MediaDatabase
17.7 MB
Total used space:
17.7 MB
Delete All Recordings
Remote recordings
Automatically retrieve remote recordings when connection is restored
Info
Settings
Streams
Record
360° Lens
Events
Client
Privacy Mask
Motion

Tareas en la pestaña Grabar

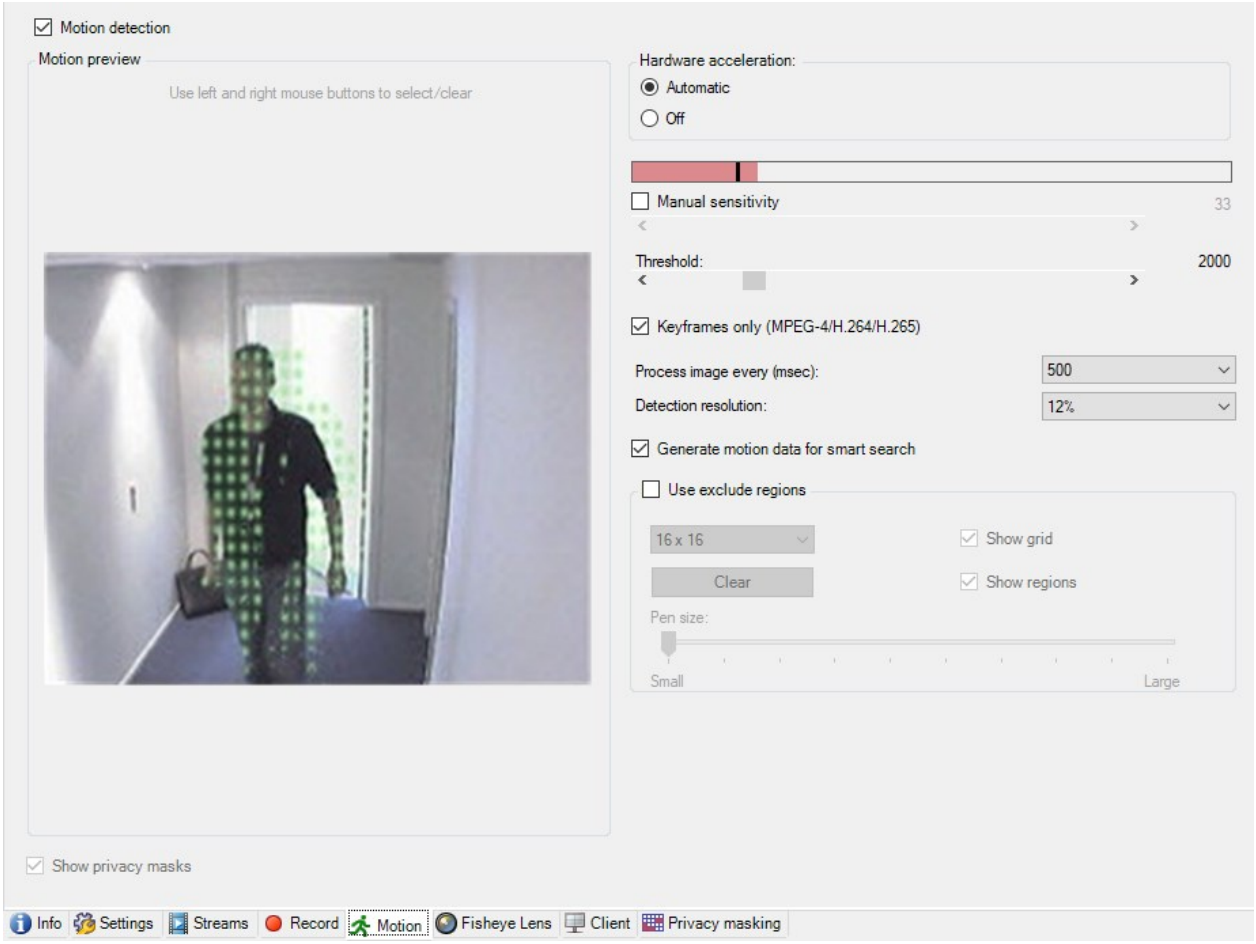
Nombre	Descripción
Grabando	Habilitar/deshabilitar la grabación Habilitar la grabación en los dispositivos relacionados
Pre-búfer	Almacenamiento en el búfer preliminar y almacenamiento de grabaciones en el búfer preliminar (explicación) Gestionar almacenamiento previo en búfer Gestionar la grabación manual
Velocidad de fotogramas para grabación	Especificar velocidad de grabación de fotogramas Habilitar la grabación de fotogramas clave
Almacenamiento	Monitorice el estado de las bases de datos para dispositivos
Seleccionar	Mover dispositivos de un almacenamiento a otro
Eliminar todas las grabaciones	Utilice este botón si ha añadido todos los dispositivos de este grupo al mismo servidor: Borrar grabaciones
Recupera automáticamente las grabaciones a distancia cuando se restaura la conexión	Guardar y recuperar grabación remota

Pestaña Movimiento (dispositivos)

Los siguientes dispositivos tienen una pestaña **Movimiento**:

- Cámaras

En la pestaña **Movimiento**, puede habilitar y configurar la detección de movimiento para la cámara seleccionada.



Tareas en la pestaña Movimiento

Nombre	Descripción
Detección de movimiento	Habilitar y deshabilitar la detección de movimiento
Aceleración de hardware	Seleccione **Automático** para habilitar la aceleración de hardware o seleccione **Desactivado** para deshabilitar el ajuste. Para obtener información adicional, consulte Habilitar o deshabilitar aceleración de hardware.
Máscaras de privacidad	Si ha definido áreas con máscaras de privacidad permanente, puede seleccionar la casilla de verificación **Máscaras de privacidad** para mostrar las máscaras de privacidad en la pestaña **Movimiento**. Defina áreas con máscaras de privacidad en

Nombre	Descripción
	Pestaña Enmascaramiento de la privacidad (dispositivos) en la página 478. No hay detección de movimiento en áreas cubiertas por máscaras de privacidad permanente.
Sensibilidad manual	Determine **cuánto cada píxel** debe cambiar en la imagen antes de que se considere movimiento: Habilitar la sensibilidad manual para definir el movimiento
Umbral	Determine **cuántos píxeles** deben cambiar en la imagen antes de que se considere como movimiento: Especificar umbral para definir movimiento
Solo fotogramas clave (MPEG-4/H.264/H.265)	Seleccione esta casilla de verificación para hacer detección de movimiento solo en fotogramas clave, en lugar de en todo el flujo de vídeo. Solo se aplica a MPEG-4/H.264/H.265. La detección de movimiento en fotogramas clave reduce la cantidad de potencia de procesamiento utilizada para realizar el análisis.
Procesar imagen cada (mseg)	Seleccione un intervalo de procesamiento de imágenes en esta lista para determinar con qué frecuencia el sistema realiza el análisis de detección de movimiento. Por ejemplo, cada 1000 milisegundos es uno cada segundo. El valor predeterminado es cada 500 milisegundos. El intervalo se aplica si la velocidad de fotogramas real es superior al intervalo que establezca aquí.
Resolución de detección	Seleccione una resolución de detección en esta lista para optimizar el rendimiento de la detección de movimiento. Solo se analiza el porcentaje seleccionado de la imagen, por ejemplo el 25 %. Al analizar el 25 %, en lugar de todos los píxeles, solo se analiza cada cuarto pixel en la imagen. El uso de la detección optimizada reduce la cantidad de potencia de procesamiento utilizada para realizar el análisis, pero también significa una detección de

Nombre	Descripción
	movimiento menos precisa.
Generar datos de movimiento para búsqueda inteligente	Con esta casilla de verificación habilitada, el sistema genera datos de movimiento para las imágenes utilizadas para la detección de movimiento. Por ejemplo, si selecciona detección de movimiento solo en fotogramas clave, el dato de movimiento también se produce solo para fotogramas clave. Los datos extra de movimiento habilitan al usuario cliente, por medio de la función de búsqueda inteligente, para realizar búsquedas rápidas de grabaciones basadas en el movimiento en el área seleccionada de la imagen. El sistema no genera datos de movimiento dentro de áreas cubiertas por máscaras de privacidad permanentes, pero sino solo para áreas con máscaras de privacidad levantables (consulte Detección de movimiento (explicación)). El umbral de detección de movimiento y las regiones de exclusión no influyen en los datos de movimiento generados. • Especifique el ajuste predeterminado de generar datos de búsqueda inteligentes para cámaras en **Herramientas** > **Opciones** > **General**.
Utilizar regiones excluidas	Excluir la detección de movimiento de áreas específicas de la vista de una cámara: Especificar regiones de exclusión para detección de movimiento

Pestaña Valores preestablecidos (dispositivos)

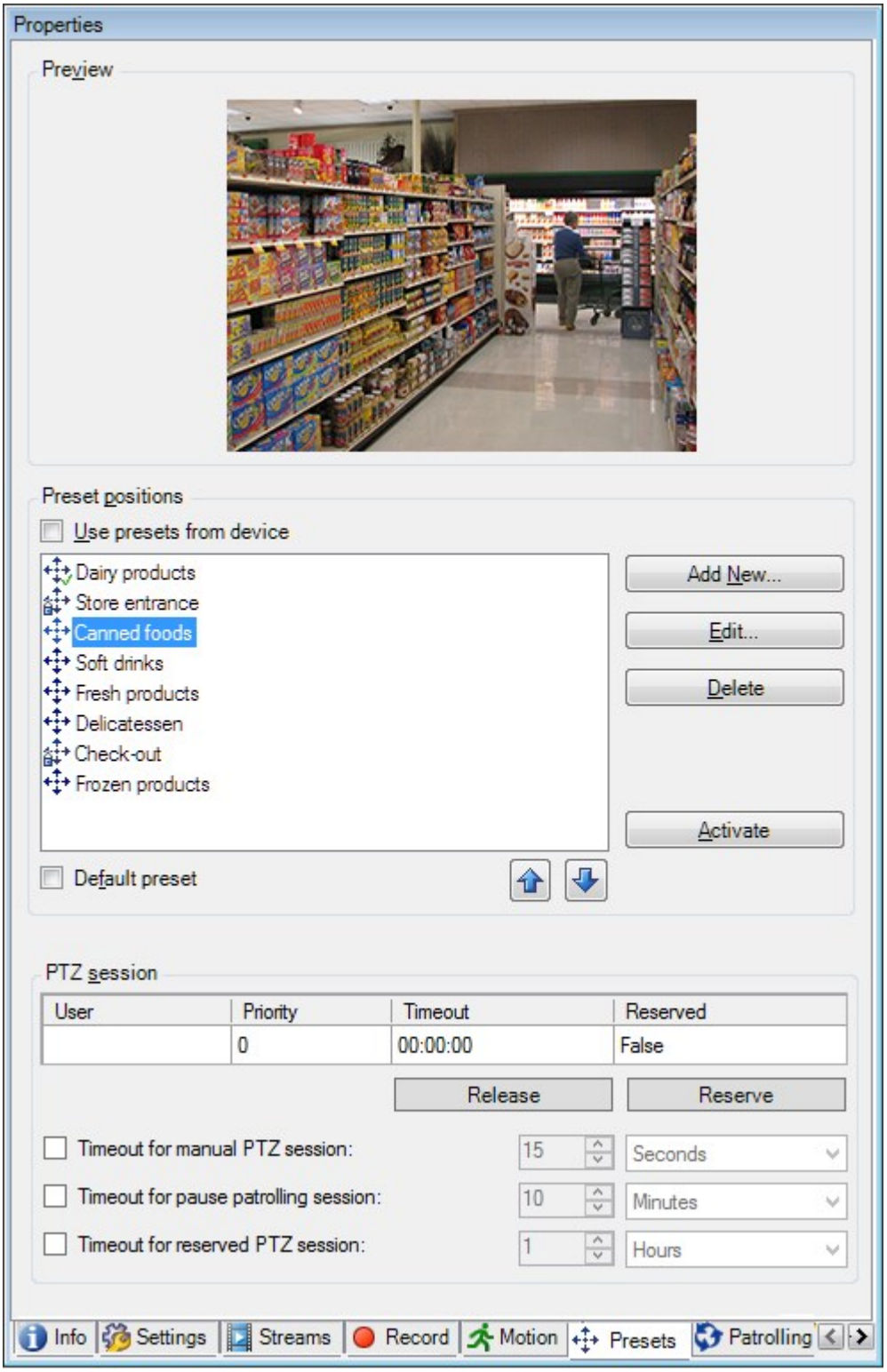
Los siguientes dispositivos tienen una pestaña **Valores preestablecidos**:

- Cámaras PTZ que admiten posiciones predefinidas

En la pestaña **Valores preestablecidos**, puede crear o importar posiciones preestablecidas, por ejemplo:

- En reglas para hacer que una cámara PTZ (panorámica-inclinación-zoom) se mueva a una posición predefinida específica cuando se produce un evento
- En vigilancia, para el movimiento automático de una cámara PTZ entre un número de posiciones predefinidas
- Para activación manual mediante el usuario XProtect Smart Client

Asigne permiso de PTZ a roles en la pestaña Seguridad general (consulte Pestaña Seguridad global (roles) en la página 540) o en la pestaña PTZ (consulte Pestaña PTZ (roles) en la página 586).


Properties
Preview
Preset positions
Use presets from device
Dairy products
Store entrance
Canned foods
Soft drinks
Fresh products
Delicatessen
Check-out
Frozen products
Add New...
Edit...
Delete
Activate
Default preset
PTZ session
User
Priority
Timeout
Reserved
0
00:00:00
False
Release
Reserve
Timeout for manual PTZ session:
15
Seconds
Timeout for pause patrolling session:
10
Minutes
Timeout for reserved PTZ session:
1
Hours
Info
Settings
Streams
Record
Motion
Presets
Patrolling

Tareas en la pestaña Valores preestablecidos

Nombre	Descripción
Nuevo	Añadir una posición predefinida para una cámara en el sistema: Añadir una posición preestablecida (tipo 1)
Utilizar valores preestablecidos del dispositivo	Añadir una posición predefinida para una cámara PTZ en la propia cámara: Utilizar posiciones predefinidas desde la cámara (tipo 2)
Valor preestablecido predeterminado	Asignar una de las posiciones predefinidas de la cámara PTZ como la posición predefinida predeterminada de la cámara: Asignar la posición preestablecida de una cámara como predeterminada
Editar	Edite una posición predefinida existente definida en el sistema: Editar una posición preestablecida para una cámara (solo tipo 1) Edite el nombre de una posición predefinida definida en la cámara: Cambiar el nombre de una posición predefinida para una cámara (solo tipo 2)
Bloqueado	Seleccione esta casilla de verificación para bloquear una posición predefinida. Puede bloquear una posición preestablecida si desea evitar que los usuarios en XProtect Smart Client o los usuarios con permisos de seguridad limitados actualicen o eliminen un valor preestablecido. Los valores preestablecidos bloqueados se indican con este icono  . Bloquea valores preestablecidos como parte de la adición (consulte Añadir una posición preestablecida [tipo 1]) y la

Nombre	Descripción
	edición (consulte Editar una posición preestablecida [solo tipo 1]).
Activar	Haga clic en este botón para probar una posición predefinida de las cámaras: Pruebe una posición predefinida (solo tipo 1y).
Reservar y **Liberar**	Evite que otros usuarios asuman el control de la cámara y liberen la reserva. Los administradores con permisos 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. Con los permisos suficientes, puede liberar las sesiones PTZ reservadas de otros usuarios: Reservar y liberar sesiones de PTZ.
Sesión PTZ	Monitorice si el sistema está vigilando actualmente o si un usuario ha tomado el control: Propiedades de la sesión de PTZ en la página 468. Ver el estado de las cámaras PTZ y los gestionar tiempos de espera para las cámaras: Especifique tiempos de espera para sesiones de PTZ.

Propiedades de la sesión de PTZ

La tabla **Sesión de PTZ** muestra el estado actual de la cámara PTZ.

Nombre	Descripción
Usuario	Muestra el usuario que ha pulsado el botón **Reservado** y actualmente controla la cámara PTZ. Si el sistema activa una sesión de vigilancia, muestra **Vigilancia**.
Prioridad	Muestra la prioridad de PTZ del usuario. Solo puede asumir sesiones de PTZ de usuarios con una prioridad inferior a la suya.
Tiempo agotado	Muestra el tiempo restante de la sesión actual de PTZ.
Reservada	Indica si la sesión actual es una sesión de PTZ reservada o no: • **Verdadero**: Reservada • **Falso**: No reservado

Las casillas de verificación en la sección **Sesión PTZ** le habilita para cambiar los siguientes tiempos de espera para cada cámara PTZ.

Nombre	Descripción
Tiempo de espera para la sesión manual de PTZ	Especifique el periodo de tiempo de espera para sesiones de PTZ manuales en esta cámara, si quiere que el tiempo de espera sea diferente del periodo predeterminado. Usted especifica el periodo predeterminado en el menú **Herramientas** en **Opciones**.
Tiempo de espera para poner en pausa la sesión de vigilancia de PTZ	Especifique el periodo de tiempo de espera para pasar las sesiones de PTZ de vigilancia en esta cámara, si quiere que el tiempo de espera sea distinto del periodo predeterminado. Usted especifica el periodo predeterminado en el menú **Herramientas** en **Opciones**.
Tiempo de	Especifique el periodo de tiempo de espera para sesiones de PTZ

Nombre	Descripción
espera para sesión de PTZ reservada	reservadas en esta cámara, si quiere que el tiempo de espera sea distinto del periodo predeterminado. Usted especifica el periodo predeterminado en el menú **Herramientas** en **Opciones**.

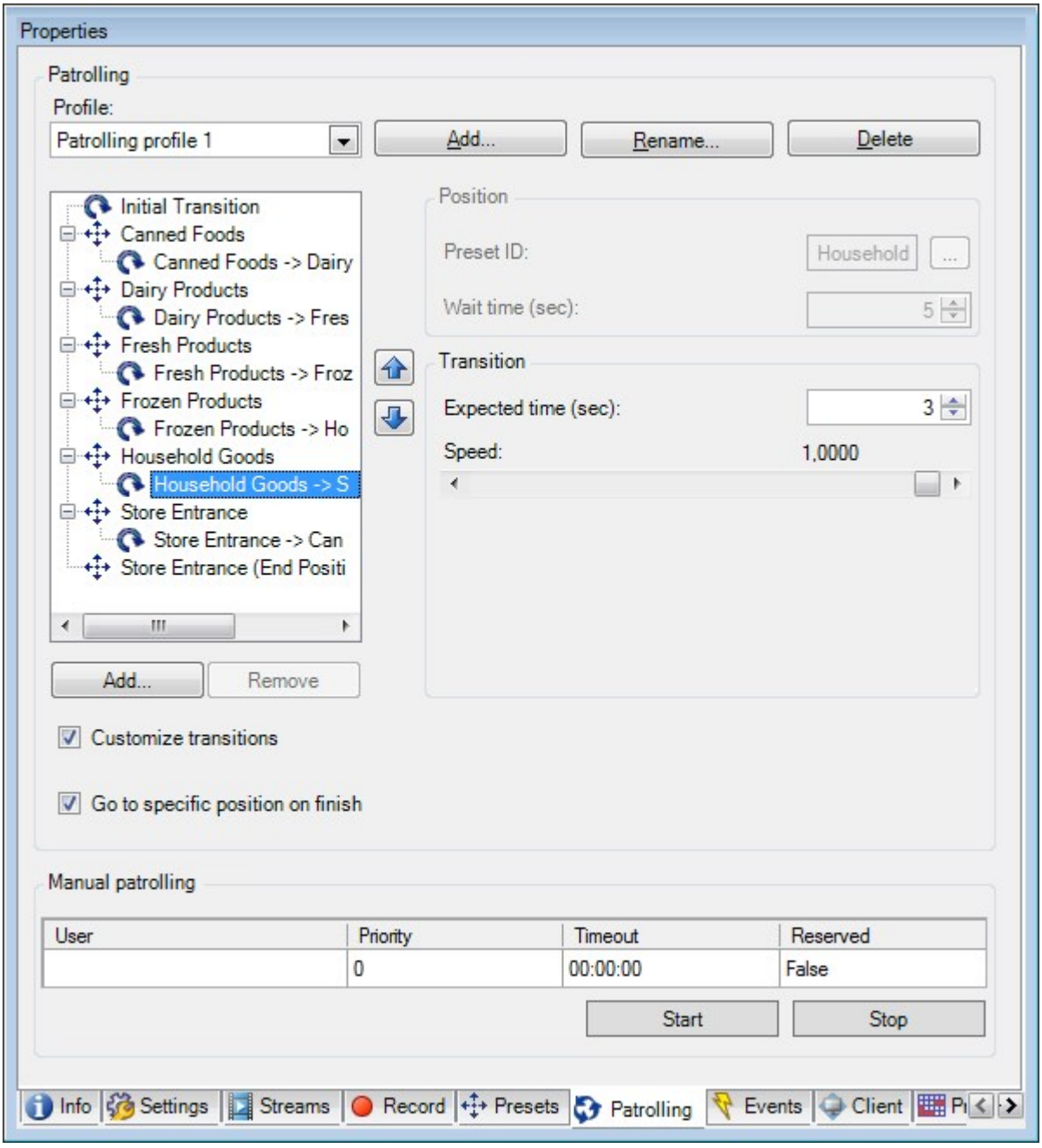
Pestaña Vigilancia (dispositivos)

Los siguientes dispositivos tienen una pestaña **Vigilancia**:

- Cámaras PTZ

En la pestaña **Vigilancia**, puede crear perfiles de vigilancia - el movimiento automático de una cámara PTZ (panorámica-inclinación-zoom) entre una serie de posiciones predefinidas.
Antes de poder trabajar con las patrullas, debe especificar al menos dos posiciones preestablecidas para la cámara en la pestaña **Valores preestablecidos**, consulte Añadir una posición preestablecida (tipo 1).

Pestaña **Vigilancia**, que muestra un perfil de vigilancia con transiciones personalizadas:


Properties
Patrolling
Profile:
Patrolling profile 1
Add...
Rename...
Delete
Initial Transition
Canned Foods
Canned Foods -> Dairy
Dairy Products
Dairy Products -> Fres
Fresh Products
Fresh Products -> Froz
Frozen Products
Frozen Products -> Ho
Household Goods
Household Goods -> S
Store Entrance
Store Entrance -> Can
Store Entrance (End Positi
Position
Preset ID:
Household
Wait time (sec):
5
Transition
Expected time (sec):
3
Speed:
1,0000
Add...
Remove
Customize transitions
Go to specific position on finish
Manual patrolling
User
Priority
Timeout
Reserved
0
00:00:00
False
Start
Stop
Info
Settings
Streams
Record
Presets
Patrolling
Events
Client

Tareas en la pestaña Vigilancia

Nombre	Descripción
Añadir	Añadir un perfil de patrulla
ID predefinido	Especificar posiciones predefinidas en un perfil de vigilancia
Tiempo de espera (s)	Especificar el tiempo en cada posición predefinida
Personalizar transiciones	Personalizar transiciones (PTZ)
Ir a una posición específica al finalizar	Especificar una posición final al realizar la vigilancia
Patrulla manual	Monitorice si el sistema está vigilando actualmente o si un usuario ha tomado el control.
Iniciar y **Parar**	Utilice los botones **Iniciar** y **Parar** para iniciar y parar manualmente la vigilancia. Consulte Especificar tiempos de espera de sesión de PTZ para obtener información sobre cómo especificar la cantidad de tiempo que debe transcurrir antes de que se reanude la vigilancia normal para todas las cámaras PTZ o para cámaras PTZ individuales.

Propiedades de vigilancia manual

La tabla **Vigilancia manual** muestra el estado actual de la cámara PTZ.

Nombre	Descripción
Usuario	Muestra el usuario que ha reservado la sesión PTZ o que inició una vigilancia manual y

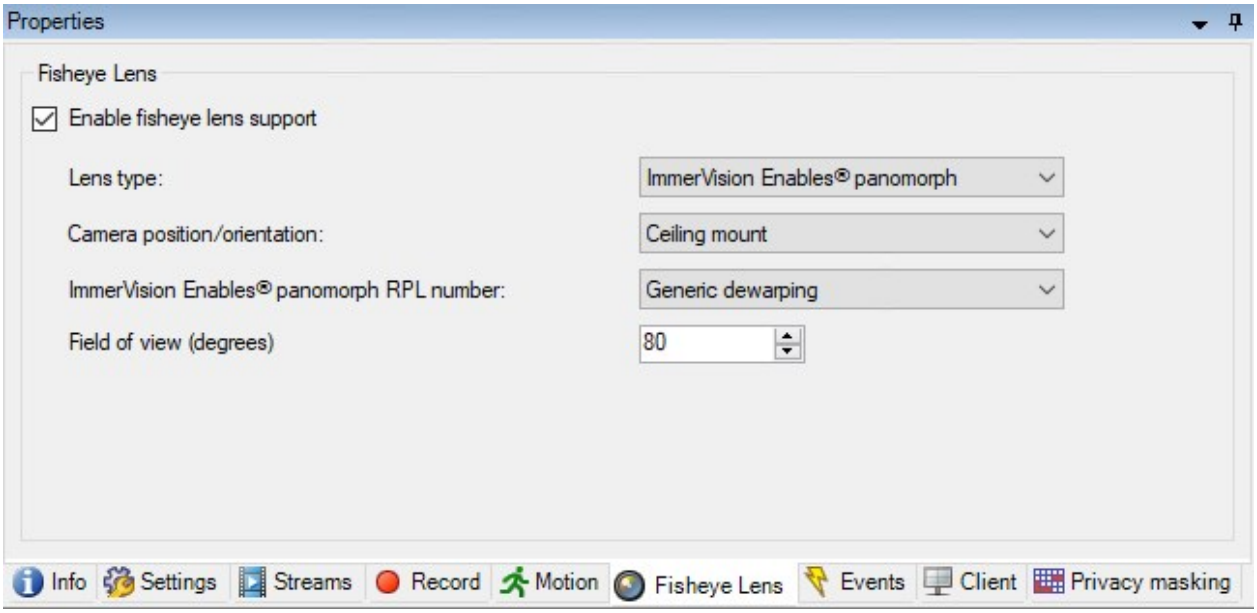
Nombre	Descripción
	controla actualmente la cámara. Si el sistema activa una sesión de vigilancia, muestra **Vigilancia**.
Prioridad	Muestra la prioridad de PTZ del usuario. Solo puede asumir sesiones de PTZ de usuarios o perfiles de vigilancia con una prioridad inferior a la suya.
Tiempo agotado	Muestra el tiempo restante de las sesiones PTZ manuales o reservadas actuales.
Reservada	Indica si la sesión actual es una sesión de PTZ reservada o no. • **Verdadero**: Reservada • **Falso**: No reservado

Pestaña Objetivo ojo de pez (dispositivos)

Los siguientes dispositivos tienen una pestaña **Objetivos ojo de pez**:

- Cámaras fijas con un objetivo ojo de pez

En la pestaña **Objetivo de ojo de pez**, puede habilitar y configurar la compatibilidad con objetivos de ojo de pez para la cámara seleccionada.



Tarea en la pestaña Objetivo ojo de pez

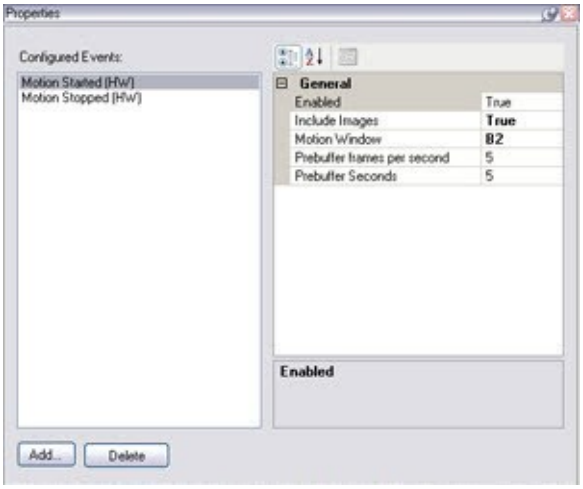
Nombre	Descripción
Habilitar soporte para ojo de pez	Habilitar y deshabilitar la compatibilidad con lentes de ojo de pez

Pestaña Eventos (dispositivos)

Los siguientes dispositivos tienen una pestaña **Eventos**:

- Cámaras
- Micrófonos
- Entradas

Además del evento del sistema, algunos dispositivos pueden configurarse para desencadenar eventos. Puede utilizar estos eventos al crear reglas basadas en eventos en el sistema. Técnicamente, ocurren en el hardware/dispositivo real en lugar de en el sistema de vigilancia.



Tareas en la pestaña Eventos

Nombre	Descripción
Añadir y **Eliminar**	Añadir o eliminar un evento para un dispositivo

Pestaña Evento (propiedades)

Nombre	Descripción
Eventos configurados	Los eventos que puede seleccionar y añadir en la lista **Eventos configurados** viene determinado íntegramente por el dispositivo y su configuración. Para algunos tipos de dispositivos, la lista está vacía.
General	La lista de propiedades depende del servicio y del evento. Para que el evento funcione según lo previsto, debe especificar algunas o todas las propiedades de forma idéntica en el dispositivo, así como en esta pestaña.

Pestaña Cliente (dispositivos)

Los siguientes dispositivos tienen una pestaña **Cliente**:

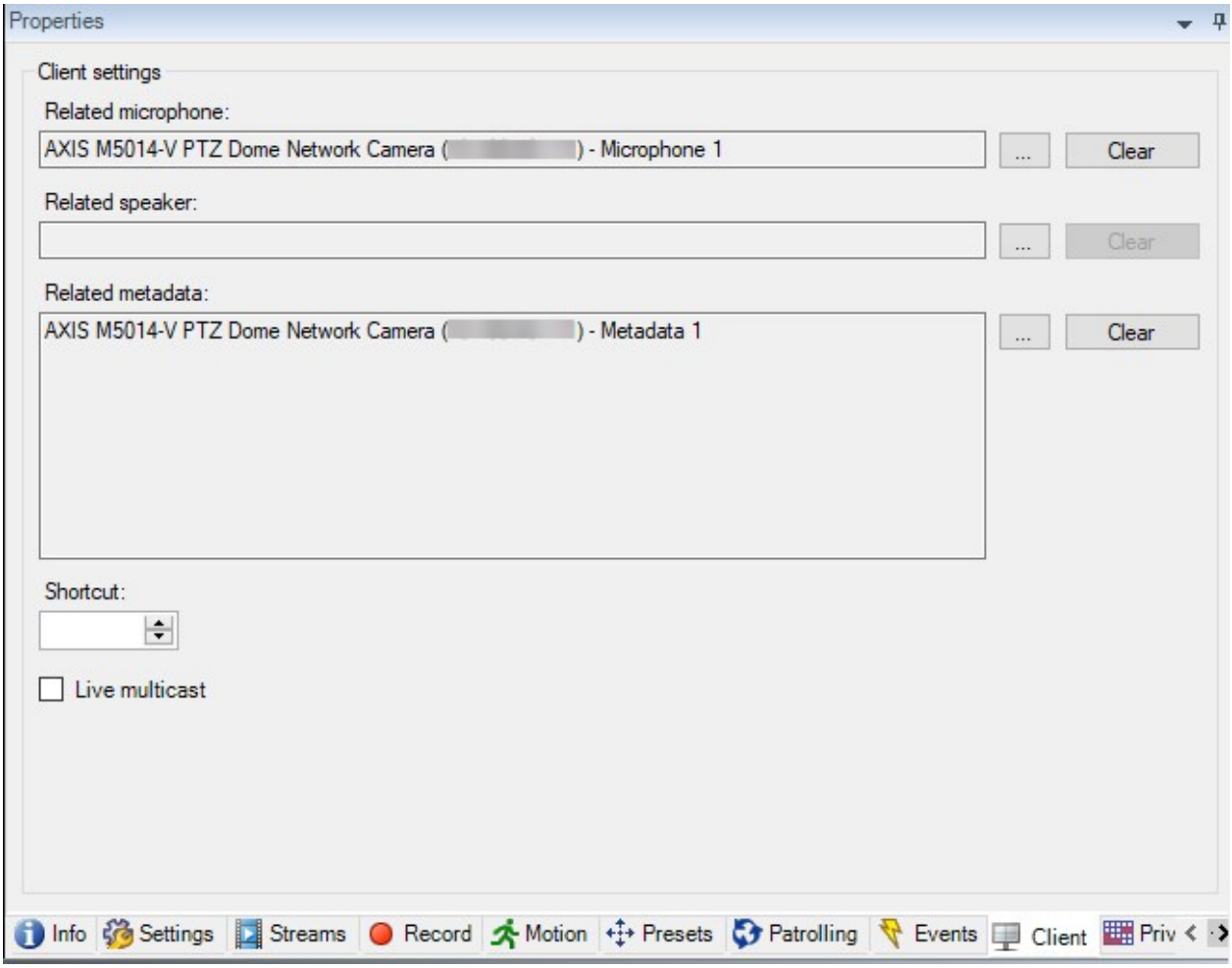
- Cámaras

En la pestaña **Cliente** puede especificar qué otros dispositivos se ven y escuchan cuando se utiliza la cámara en XProtect Smart Client.

Los dispositivos relacionados también graban cuando la cámara graba, consulte Habilitar la grabación en los dispositivos relacionados en la página 235.

También puede habilitar **Multidifusión en directo** en la cámara. Significa que la cámara realiza la multidifusión de flujos en directo a los clientes por medio del servidor de grabaciones.

Los flujos de multidifusión no están cifrados, aunque el servidor de grabación utilice el cifrado.



Propiedades de la pestaña Cliente

Nombre	Descripción
Micrófono relacionado	Especifique el micrófono de la cámara en el que los usuarios de XProtect Smart Client escuchan el audio de forma predeterminada. El usuario de XProtect Smart Client puede seleccionar manualmente escuchar otro micrófono en caso necesario. Especifique el micrófono que está relacionado con la cámara de envío automático de vídeo para transmitir vídeo con audio.

Nombre	Descripción
	Los micrófonos relacionados graban cuando la cámara graba.
Altavoz relacionado	Especifique a través de qué altavoces de la cámara hablarán los usuarios de XProtect Smart Client de forma predeterminada. El usuario de XProtect Smart Client puede seleccionar manualmente otro altavoz en caso necesario. Los altavoces relacionados graban cuando la cámara graba.
Metadatos relacionados	Especifique uno o más dispositivos de metadatos en la cámara, de los que los usuarios de XProtect Smart Client reciben datos. Los dispositivos de matetadatos relacionados graban cuando la cámara graba.
Acceso rápido	Para facilitar la selección de cámaras para los usuarios de XProtect Smart Client, defina métodos abreviados del teclado para la cámara. • Crear cada método abreviado de modo que identifique de forma única la cámara • El número de acceso directo de una cámara no puede tener más de cuatro dígitos
Multidifusión en directo	El sistema admite multidifusión de flujos en directo desde el servidor de grabaciones a XProtect Smart Client. Para habilitar la multidifusión de flujos en directo desde la cámara, seleccione la casilla de verificación. La multidifusión en directo solo funciona en la transmisión que ha especificado como el flujo predeterminado de la cámara en la pestaña **Flujos**. También debe configurar la multidifusión para el servidor de grabaciones. Consulte Habilitar la multidifusión para el servidor de grabación en la página 210. Los flujos de multidifusión no están cifrados, aunque el servidor de grabación utilice el cifrado.

Pestaña Enmascaramiento de la privacidad (dispositivos)

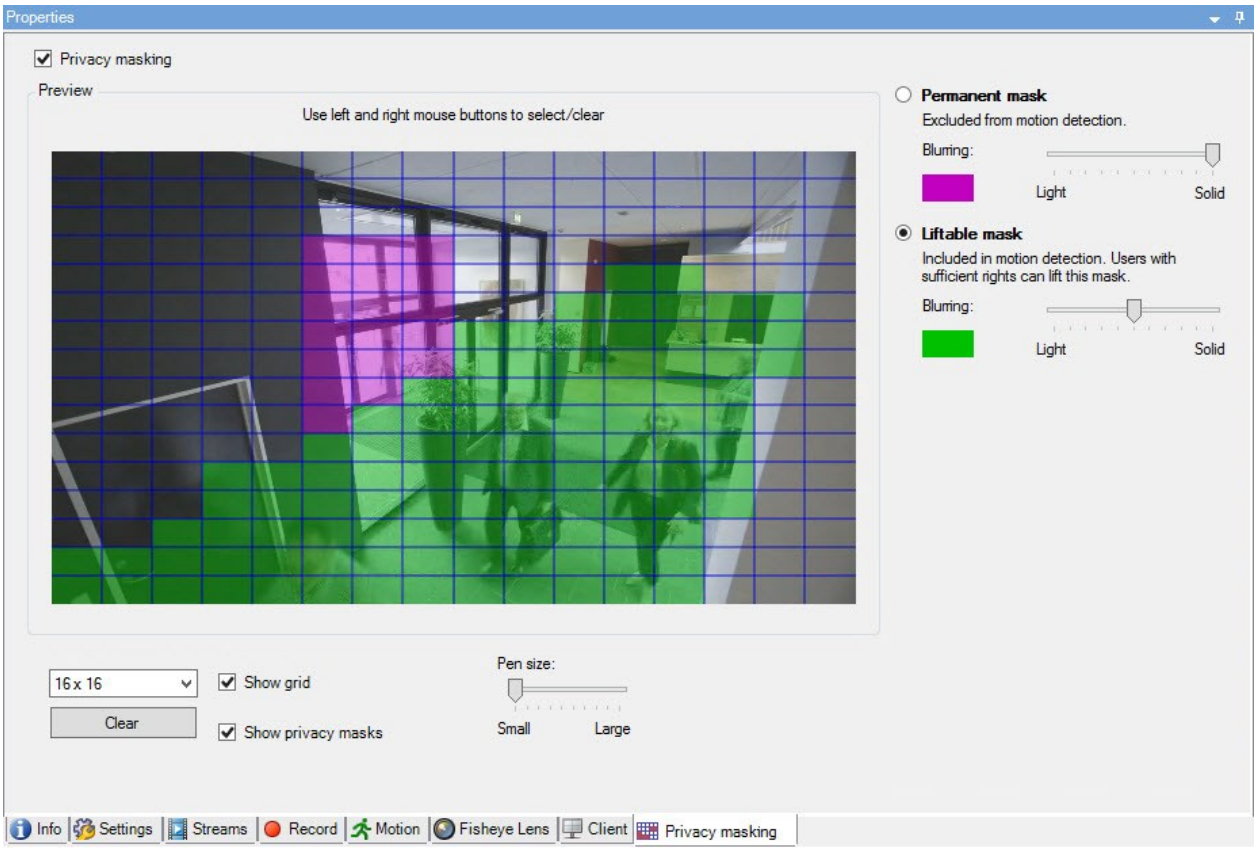
> La funcionalidad disponible depende del sistema que esté utilizando. Vea la lista completa de características, que está disponible en la página de descripción del producto en el sitio web Milestone (https://www.milestonesys.com/solutions/platform/product-index/).

XProtect Essential+ 2018 R1 y en adelante no admite la máscara de privacidad, por lo que si se actualiza desde un sistema con máscaras de privacidad aplicadas, las máscaras se eliminarán.

Los siguientes dispositivos tienen una pestaña **Enmascaramiento de la privacidad**:

- Cámaras

En la pestaña **Enmascaramiento de privacidad**, puede habilitar y configurar la protección de la privacidad para la cámara seleccionada.



Tareas en la pestaña Enmascaramiento de la privacidad

Nombre	Descripción
Máscara de privacidad	Habilitar/deshabilitar la máscara de privacidad Máscara de privacidad (explicación)
Máscara permanente y **Máscara levantable**	Defina si quiere una máscara de privacidad permanente o levantable: Definir las máscaras de privacidad

Tareas relacionadas con el Enmascaramiento de la privacidad

Tarea	Descripción
Cambie el tiempo de espera para las máscaras de privacidad levantadas para el perfil Smart Client asociado al rol que tiene el permiso para levantar máscaras de privacidad.	Cambiar el tiempo de espera de las máscaras de privacidad levantadas
Habilite o deshabilite el permiso para levantar máscaras de privacidad para un rol.	Dar permiso a los usuarios para levantar las máscaras de privacidad
Cree un informe de dispositivos con unformación sobre los ajustes actuales de mascaras de privacidad de sus cámaras.	Crear un informe de su configuración de máscara de privacidad

Pestaña Enmascaramiento de la privacidad (propiedades)

Nombre	Descripción
Tamaño de la cuadrícula	El tamaño de cuadrícula seleccionado determina la densidad de la cuadrícula, independientemente de si la cuadrícula es visible en la vista previa o no. Seleccione entre los valores 8×8, 16×16, 32×32 o 64×64.
Limpiar	Desactiva **todas** las máscaras de privacidad que ha especificado.
Mostrar cuadrícula	Seleccione la casilla de verificación **Mostrar cuadrícula** para hacer que la cuadrícula sea visible.
Mostrar máscaras de privacidad	Al seleccionar la casilla de verificación **Mostrar máscaras de privacidad** (predeterminado), las máscaras de privacidad permanentes aparecen en morado en la vista previa y las máscaras de privacidad levantables aparecen en verde. Milestone recomienda que mantenga seleccionado el cuadro **Mostrar mascaras de privacidad** para que usted y sus colegas puedan ver la configuración actual de protección de la privacidad.
Tamaño del lápiz	Utilice el control deslizante **Tamaño del lápiz** para indicar el tamaño de las selecciones que desea hacer cuando haga clic y arrastre la cuadrícula para seleccionar regiones. El valor predeterminado se ha definido en pequeño, que es equivalente a un cuadrado de la cuadrícula.
Máscara permanente	Aparece en morado en la vista previa de esta pestaña y en la pestaña **Movimiento**. Las máscaras de privacidad permanente siempre están visibles en XProtect Smart Client y no pueden levantarse. Se puede usar para cubrir áreas del vídeo que nunca requieren vigilancia, como áreas públicas en las que no está permitida la vigilancia. La detección de movimiento se ha excluido de las máscaras permanentes. Especifique la cobertura de las máscaras de la privacidad como sólida o algún nivel de difuminado. Los ajustes de cobertura se aplican tanto al vídeo en directo como grabado.
Máscara elevable	Aparece en verde en la vista de previa de esta pestaña. Las máscaras de privacidad levantables pueden ser levantadas en XProtect Smart Client por los usuarios con suficientes permisos de usuario. De forma predeterminada, las máscaras de privacidad se levantan durante 30 minutos o hasta que el usuario las

Nombre	Descripción
	vuelva a aplicar. Esté atento a que las máscaras de privacidad se levanten en el vídeo desde todas las cámaras a las que el usuario tiene acceso. Si el usuario de XProtect Smart Client no tiene permiso para levantar las máscaras de privacidad, el sistema pregunta por un usuario con permiso para autorizar el levantamiento. Especifique la cobertura de las máscaras de privacidad, ya sea sólida o un nivel de difuminación. Los ajustes de cobertura se aplican tanto al vídeo en directo como grabado.
Desenfoque	Utilice el control deslizante para seleccionar el nivel de difuminado de las máscaras de la privacidad en los clientes o establezca la cobertura de sólido. De forma predeterminada, la cobertura de áreas con máscaras de privacidad permanente es sólida (no transparente). De forma predeterminada, las máscaras de privacidad elevables están medio desenfocadas. Puede informar a los usuarios clientes sobre el aspecto de máscaras de privacidad permanentes y levantables, para que puedan distinguirlas.

Ventana de propiedades de hardware

Tiene varias opciones para añadir hardware a cada servidor de grabación de su sistema.

> ⚠ Si su hardware se encuentra detrás de un router con NAT o de un cortafuegos, es posible que tenga que especificar un número de puerto diferente y configurar el router/cortafuegos de forma que planifique el puerto y las direcciones IP que utiliza el hardware.

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

Pestaña Información (hardware)

Para obtener información sobre la pestaña **Información** para servidores remotos, consulte Pestaña Información (servidor remoto) en la página 447.

Nombre	Descripción
Nombre	Introduzca un nombre. El sistema utiliza el nombre siempre que el hardware esté recogido en el sistema y en los clientes. No es necesario que el nombre sea único. Al cambiar el nombre de hardware, el nombre cambia globalmente en Management Client.
Descripción	Introduzca una descripción del hardware (opcional). La descripción aparece en varios listados del sistema. Por ejemplo, al mover el puntero del ratón por el nombre del hardware en el panel **Descripción general**: 
Modelo	Identifica el modelo de hardware.
Número de serie	Número de serie de hardware según lo especificado por el fabricante. Con frecuencia, pero no siempre, el número de serie es idéntico a la dirección MAC.
Controlador	Identifica el controlador que controla la conexión con el hardware.
IE	Abre la página de inicio predeterminada del proveedor de hardware. Puede utilizar esta página para la administración del hardware.
Dirección	El nombre del host o la dirección IP del hardware.
Dirección MAC	Especifica la dirección de Control de acceso a medios (Media Access Control, MAC) del hardware del sistema. Una dirección MAC es un número hexadecimal de 12 caracteres que identifica de forma única cada elemento de hardware de una red.
Versión de firmware:	La versión del firmware del dispositivo de hardware. Para asegurarse de que el sistema muestra la versión actual, ejecute el asistente de **Actualización de datos de hardware** después de cada actualización del firmware.
Último cambio de contraseña:	El campo **Último cambio de contraseña** muestra la fecha y hora del último cambio de contraseña según la configuración de la hora local del ordenador desde el que se cambió la contraseña.

Nombre	Descripción
Datos del hardware actualizados por última vez:	Hora y fecha de la última actualización de los datos del hardware.

Pestaña Ajustes (hardware)

En la pestaña **Ajustes**, puede verificar o editar ajustes para el hardware.

> El contenido de la pestaña **Ajustes** viene determinada por el hardware seleccionado, y varía dependiendo del tipo de hardware. Para algunos tipos de hardware, la pestaña **Ajustes** no muestra contenido en absoluto o contenido de solo lectura.

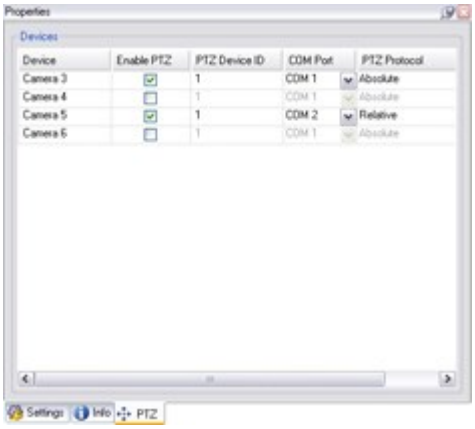
Para obtener información sobre la pestaña **Ajustes** para servidores remotos, consulte Pestaña Ajustes (servidor remoto) en la página 448.

Pestaña PTZ (codificadores de vídeo)

En la pestaña **PTZ**, puede habilitar PTZ (panorámica-inclinación-zoom) para codificadores de vídeo. La pestaña está disponible si el dispositivo seleccionado es un codificador de vídeo o si el controlador admite tanto cámaras PTZ como cámaras no 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 que pueda utilizar las funciones de PTZ de las cámaras PTZ conectadas al codificador de vídeo.

> No todos los codificadores de vídeo admiten el uso de cámaras PTZ. Aunque los codificadores de vídeo puedan admitir el uso de cámaras PTZ, puede requerir configuración antes de poder usar las cámaras PTZ. Es normalmente la instalación de controladores adicionales mediante una interfaz de configuración basada en el explorador en la dirección IP del dispositivo.



Pestaña **PTZ**, con PTZ habilitado para dos canales en un codificador de vídeo.

Nodo cliente

Clientes (nodo)

Este artículo describe cómo personalizar la interfaz de usuario para operadores en XProtect Smart Client y para administradores del sistema en Management Client.

Smart Wall (nodo Cliente)

Smart Wall propiedades

Pestaña de información

En la pestaña **Información** de una definición de Smart Wall, puede añadir y editar propiedades Smart Wall.

Nombre	Descripción
Nombre	El nombre de la definición Smart Wall. Visualizado en XProtect Smart Client como el Smart Wall nombre del grupo de la vista.
Descripción	Una descripción de la definición Smart Wall. La descripción solo se utiliza internamente en XProtect Management Client.
Texto de estado	Muestra la información del estado de la cámara y del sistema en los elementos de la vista de la cámara.

Nombre	Descripción
Sin barra de título	Oculta la barra de título en todos los elementos de la vista en el panel de vídeo.
Barra de título	Mostrar la barra de título en todos los elementos de la vista en el panel de vídeo.

Pestaña valores preestablecidos

En la pestaña **Valores preestablecidos** para una definición de Smart Wall, puede añadir y editar Smart Wallvalores preestablecidos[1].

Nombre	Descripción
Añadir nuevo	Añade un valor preestablecido a su definición Smart Wall. Introduce un nombre y una descripción para el valor preestablecido.
Editar	Edita el nombre o la descripción de un valor preestablecido.
Borrar	Elimina un valor preestablecido.
Activar	Aplicar el valor preestablecido en los monitores Smart Wall que están configurados para utilizar el valor preestablecido. Para aplicar un valor preestablecido automáticamente, debe crear una regla que utilice el valor preestablecido.

Pestaña de distribución

En la pestaña **Distribución** de una definición Smart Wall, posiciona los monitores, de modo que sus posiciones se asemejen al montaje de los monitores físicos en el panel de vídeo. La distribución también se utiliza en XProtect Smart Client.

[1]Disposición predefinida para uno o varios monitores Smart Wall en XProtect Smart Client. Los valores preestablecidos determinan qué cámaras se muestran y cómo se estructura el contenido en cada monitor del panel de vídeo.

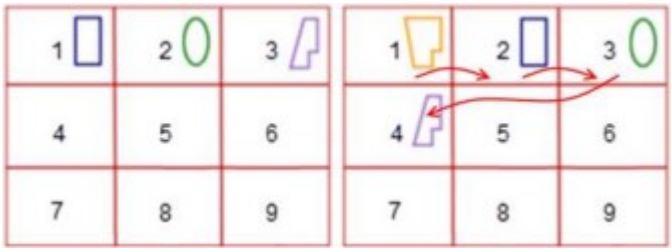
Nombre	Descripción
Editar	Ajustar el posicionamiento de los monitores.
Movimiento	Para mover un monitor a una nueva posición, seleccione el monitor y arrástrelo a la posición deseada, o haga clic en uno de los botones de flecha para mover el monitor en la dirección seleccionada.
Botones de zoom	Acerque o aleje la vista previa de la distribución Smart Wall para asegurarse de que coloca los monitores correctamente.
Nombre	El nombre del monitor. El nombre se muestra en XProtect Smart Client.
Tamaño	El tamaño del monitor físico en el panel de vídeo.
Relación de aspecto	La relación altura/anchura del monitor físico en el panel de vídeo.

Propiedades del monitor

Pestaña de información

En la pestaña **Información** para el monitor en un valor preestablecido Smart Wall puede añadir monitores y editar la configuración de los mismos.

Nombre	Descripción
Nombre	El nombre del monitor. El nombre se muestra en XProtect Smart Client.
Descripción	Una descripción del monitor. La descripción sólo se utiliza internamente en el archivo XProtect Management Client.
Tamaño	El tamaño del monitor físico en el panel de vídeo.
Relación de aspecto	La relación altura/anchura del monitor físico en el panel de vídeo.

Nombre	Descripción
Valor preestablecido vacío	Define lo que debe mostrarse en un monitor con un diseño preestablecido vacío cuando se activa o selecciona un nuevo Smart Wall valor preestablecido en XProtect Smart Client: • Seleccione **Conservar** para mantener el contenido actual en el monitor. • Seleccione **Borrar** para eliminar todo el contenido y que no aparezca nada en el monitor.
Elemento preestablecido vacío	Define lo que debe mostrarse en un elemento vacío preestablecido cuando se activa o selecciona un nuevo valor preestablecido Smart Wall en XProtect Smart Client: • Seleccione **Conservar** para mantener el contenido actual en el elemento de diseño. • Seleccione **Borrar** para borrar el contenido y que no se muestre nada en el elemento de diseño.
Inserción de elementos	Define cómo se insertan las cámaras en la disposición del monitor cuando se ven en el XProtect Smart Client: • **Independiente**: sólo cambia el contenido del elemento de la distribución afectado, el resto del contenido de la distribución sigue siendo el mismo. • **Enlazado**: los contenidos de los elementos de distribución se empujan de izquierda a derecha. Si, por ejemplo, se inserta una cámara en la posición 1, la cámara anterior de la posición 1 se empuja a la posición 2, la cámara anterior de la posición 2 se empuja a la posición 3, y así sucesivamente. llustrado en este ejemplo: 

Pestaña valores preestablecidos

En la pestaña **Valores preestablecidos** para un monitor en un valor preestablecido Smart Wall, puede editar la distribución de vista y el contenido del monitor en el valor preestablecido seleccionado Smart Wall.

Nombre	Descripción
Posición prestablecida	Una lista de valores preestablecidos de Smart Wall para la definición seleccionada de Smart Wall.
Editar	Haga clic en **Editar** para editar el diseño y el contenido del monitor seleccionado. Haga doble clic en una cámara para eliminarla. Haga clic en **Borrar** para definir un nuevo diseño o para excluir el monitor en el valor preestablecido Smart Wall para que el monitor esté disponible para otros contenidos no controlados por el valor preestablecido Smart Wall. Haga clic en  para seleccionar el diseño que desea utilizar con su monitor, y haga clic en **Aceptar**.

Smart Client Perfiles (nodo Cliente)

La funcionalidad disponible depende del sistema que esté utilizando. Vea la lista completa de características, que está disponible en la página de descripción del producto en el sitio web Milestone (https://www.milestonesys.com/solutions/platform/product-index/).

En las pestañas siguientes podrá especificar las propiedades de cada perfil de Smart Client. Puede bloquear los ajustes en el Management Client en caso necesario, de modo que los usuarios de XProtect Smart Client no pueden cambiarlos.

Para crear o editar Smart Client perfiles, expanda **Cliente** y seleccione **Smart Client Perfiles**.

Pestaña Información (perfiles de Smart Client)

Esta pestaña le permite especificar las siguientes propiedades:

Pestaña	Descripción
Información	Nombre y descripción, prioridad de perfiles existentes y una descripción general de qué roles utilizan el perfil. Si un usuario es miembro de más de un rol, cada uno con su perfil individual de Smart Client, el usuario consigue el perfil de Smart Client con la máxima prioridad.

Pestaña General (perfiles de Smart Client)

Esta pestaña le permite especificar las siguientes propiedades:

Pestaña	Descripción
General	Ajustes, como mostrar/ocultar y minimizar y maximizar ajustes del menú, iniciar/cerrar sesión, inicio, tiempo de espera, información y opciones de mensajería, y habilitar o deshabilitar ciertas pestañas en XProtect Smart Client. Los ajustes **Mensajes de error de la cámara**, **Mensajes de error del servidor** y **Mensaje de error de vídeo en directo** le permiten controlar si estos mensajes de error se muestran como superposición, como imagen en negro con superposición o si se ocultan. El **mensaje Vídeo en directo detenido** se muestra en XProtect Smart Client cuando se detiene la entrada en directo de la cámara. Por ejemplo, si la cámara ha dejado de enviar imágenes, aunque esté conectada. ⚠ Si **Oculta** los mensajes de error de cámara, existe el riesgo de que el operador pase por alto que se ha perdido la conexión con una cámara. El ajuste **Cámaras permitidas durante la búsqueda** le permite controlar el número de cámaras que el operador puede añadir a las búsquedas en XProtect Smart Client. Configurar un límite de la cámara puede ayudarle a prevenir la sobrecarga del sistema. El ajuste de **Ayuda en línea** le permite desactivar el sistema de ayuda en XProtect Smart Client. El ajuste de **Tutoriales de vídeo** le permite desactivar el botón de **Tutoriales de vídeo** en XProtect Smart Client. El botón redirige a los operadores a la página de tutoriales en vídeo: https://www.milestonesys.com/support/help-yourself/video-tutorials/

Pestaña Avanzados (perfiles de Smart Client)

Esta pestaña le permite especificar las siguientes propiedades:

Pestaña	Descripción
Avanzados	Ajustes avanzados, como el número máximo de subprocesos de decodificación, desentrelazado y ajuste de zona horaria. **Máximos subprocesos de decodificación** controla la cantidad de subprocesos de decodificación que se utilizan para decodificar flujos de vídeo. También ayuda a mejorar el rendimiento en ordenadores multinúcleo en directo, así como en modo de reproducción. La mejora de rendimiento exacto depende del flujo de vídeo. Esto es principalmente relevante si se utilizan flujos de datos de vídeo de alta resolución muy codificados, como H.264/H.265, para los que el potencial de mejora de rendimiento puede ser significativo, y menos relevante si se usa, por ejemplo, JPEG o MPEG-4. Con el **desentrelazado**, se convierte vídeo a un formato no entrezalado. El entrelazado determina cómo se actualiza una imagen en la pantalla. La imagen se actualiza escaneando primero las líneas impares en la imagen, escaneando después las líneas pares. Esto permite una mayor velocidad de actualización, ya que en cada escaneo se debe procesar menos información. Sin embargo, el entrelazado puede causar un parpadeo, o los cambios en la mitad de las líneas de la imagen pueden ser notables. **Transmisión adaptativa** habilita XProtect Smart Client para que seleccione automáticamente los flujos de vídeo en directo con la mejor coincidencia de resolución para los flujos solicitados por el elemento de la vista. Esto reduce la carga en la CPU y la GPU, lo que mejora la capacidad de decodificación y el rendimiento del ordenador. Esto requiere transmisión múltiple de flujos de vídeo en directo con la configuración de distintas resoluciones, consulte Gestionar transmisiones múltiples. El streaming adaptativo puede aplicarse tanto en el modo en directo como en el modo reproducción. En el modo reproducción, el streaming adaptativo se denomina reproducción adaptativa. La reproducción adaptativa requiere que se configuren dos transmisiones para la grabación. Para obtener más información sobre cómo añadir transmisiones para el streaming adaptable en modo directo y para reproducción adaptativa, consulte Añadir un flujo en la página 238.

Pestaña Directo (perfiles de Smart Client)

Esta pestaña le permite especificar las siguientes propiedades:

Pestaña	Descripción
Directo	Disponibilidad del modo directo y otras funciones de directo, reproducción de cámaras, botones de sobreposición de cámaras y cuadros delimitadores, y también plug-ins de MIP relacionados con el directo.

Pestaña Reproducción (perfiles de Smart Client)

Esta pestaña le permite especificar las siguientes propiedades:

Pestaña	Descripción
Reproducción	Disponibilidad de modo reproducción y otras funciones de reproducción, diseño de informes impresos, reproducción independiente, marcadores y cuadros delimitadores, y también plug-ins de MIP relacionados con la reproducción.

Pestaña Configuración (perfiles de Smart Client)

Esta pestaña le permite especificar las siguientes propiedades:

Pestaña	Descripción
Ajustes	Disponibilidad de la configuración general/paneles/botones, plug-in MIP relacionado con la configuración y permisos para editar un plano y para editar el buffering de vídeo en directo.

Pestaña Exportaciones (perfiles de Smart Client)

Esta pestaña le permite especificar las siguientes propiedades:

Pestaña	Descripción
Exportar	Rutas, máscaras de privacidad, formatos de video e imágenes fijas y qué incluir al exportarlos, formatos de exportación para XProtect Smart Client – Player y mucho más.

Pestaña Línea de timepo (perfiles de Smart Client)

Esta pestaña le permite especificar las siguientes propiedades:

Pestaña	Descripción
Línea temporal	Si incluir o no audio, la visibilidad de la indicación de tiempo y movimiento, y finalmente cómo manejar las lagunas de reproducción. También puede seleccionar si mostrar o no datos adicionales o marcadores adicionales desde otras fuentes.

Pestaña Control de acceso (perfiles de Smart Client)

Esta pestaña le permite especificar las siguientes propiedades:

Pestaña	Descripción
Control de acceso	Seleccione si las notificaciones de solicitud de acceso deben aparecer en la pantalla XProtect Smart Client cuando se desencadenan mediante eventos.

Pestaña Gestor de alarmas (perfiles de Smart Client)

Esta pestaña le permite especificar las siguientes propiedades:

Pestaña	Descripción
Gestor de alarma	Especificar si:

Pestaña	Descripción
	• Las notificaciones de escritorio para alarmas deben mostrarse en ordenadores en los que XProtect Smart Client está instalado. Las notificaciones solo aparecen si XProtect Smart Client se está ejecutando, incluso si está minimizado  Las notificaciones de escritorio para alarmas aparecen solo cuando las alarmas tienen ciertas prioridades, por ejemplo, **Media** o **Alta**. Para configurar qué prioridades de alarma desencadenan notificaciones, vaya a **Alarmas** > **Ajustes de datos de alarmas** > **Niveles de datos de alarmas**. Para cada prioridad de alarma requerida, seleccione la casilla de verificación **Habilitar notificaciones de escritorio**. Consulte Ajustes de datos de alarmas (nodo Alarmas). • Las alarmas deben emitir notificaciones acústicas en los ordenadores en los que XProtect Smart Client está instalado. Las notificaciones de sonido solo se reproducen si XProtect Smart Client se está ejecutando, aunque sea minimizado  Las notificaciones acústicas para alarmas solo se reproducen cuando se asocia un sonido a la alarma. Para asociar sonidos con alarmas, vaya a **Alarmas** > **Ajustes de datos de alarmas** > **Niveles de datos de alarmas**. Para cada prioridad de alarma requerida, seleccione el sonido que se debe asociar a la alarma. Consulte Ajustes de datos de alarmas (nodo Alarmas).

Pestaña Plano inteligente (perfiles de Smart Client)

Esta pestaña le permite especificar las siguientes propiedades:

Pestaña	Descripción
Plano inteligente	Especifique los ajustes para la función de plano inteligente.

Pestaña	Descripción
	Puede especificar si: • Milestone Map Service está disponible para usar como un fondo geográfico • OpenStreetMaps está disponible para usar como un fondo geográfico • XProtect Smart Client creará automáticamente ubicaciones en las que un usuario añade una superposición personalizada al plano inteligente. También puede especificar la frecuencia con la que quiere que el sistema elimine datos relacionados con planos inteligentes desde su ordenador. Para ayudar a XProtect Smart Client a mostrar el plano inteligente más rápido, el cliente guarda datos del plano en la caché del ordenador. Con el tiempo esto podría ralentizar su ordenador. El almacenamiento en caché no se aplica a Google Maps. Si quiere utilizar Bing Maps o Google Maps como fondos geográficos, introduzca una clave de Bing Maps API o una clave de Maps Static API desde Google.

Management Client Perfiles (nodo Cliente)

La funcionalidad disponible depende del sistema que esté utilizando. Vea la lista completa de características, que está disponible en la página de descripción del producto en el sitio web Milestone (https://www.milestonesys.com/solutions/platform/product-index/).

Pestaña Información (Management Client Perfiles)

En la pestaña **Información**, puede establecer lo siguiente para los perfiles de Management Client:

Componente	Requisito
Nombre	Introduzca un nombre para el perfil Management Client.
Prioridad	Utilice las flechas arriba y abajo para establecer una prioridad para el perfil de Management Client.

Componente	Requisito
Descripción	Introduzca una descripción para el perfil. Esto es opcional.
Roles que utilizan el perfil de Management Client	Este campo muestra los roles que tiene asociados al perfil Management Client. No puede editar esto.

Pestaña Perfil (Perfiles de Management Client)

> La funcionalidad disponible depende del sistema que esté utilizando. Vea la lista completa de características, que está disponible en la página de descripción del producto en el sitio web Milestone (https://www.milestonesys.com/solutions/platform/product-index/).

En la pestaña **Perfil**, puede habilitar o deshabilitar la visibilidad de los siguientes elementos en la interfaz de usuario deManagement Client:

Navegación

En esta sección, decida si un usuario administrador asociado al perfil de Management Client tiene permiso para ver las distintas características y la funcionalidad ubicada en el panel **Navegación**.

Elemento de navegación	Descripción
Conceptos básicos	Permite al usuario administrador asociado al perfil de Management Client ver **Información de licencia** e **Información del sitio**.
Servicios de conexión remota	Permite al usuario administrador asociado al perfil de Management Client ver **Axis One-click Camera Connection**.
Servidores	Permite al usuario administrador asociado al perfil de Management Client ver **Servidores de grabación** y **Servidores de failover**.

Elemento de navegación	Descripción
Dispositivos	Permite al usuario administrado asociado al perfil de Management Client ver **Cámaras**, **Micrófonos**, **Altavoces**, **Metadatos**, **Entrada** y **Salida**.
Cliente	Permite al usuario administrador asociado al perfil de Management Client ver **Smart Wall**, **Grupos de vistas**, **Perfiles de Smart Client**, **Perfiles de Management Client** y **Matrix**.
Reglas y eventos	Permite al usuario administrador asociado al perfil de Management Client ver **Reglas**, **Perfiles temporales**, **Perfiles de notificación**, **Eventos definidos por el usuario**, **Eventos de análisis** y **Eventos genéricos**.
Seguridad	Permite al usuario administrador asociado al perfil de Management Client ver **Roles** y **Usuarios básicos**.
Panel del sistema	Permite al usuario administrador asociado al perfil de Management Client ver **Monitor del sistema**, **Umbrales del monitor del sistema**, **Bloqueo de evidencias**, **Tareas actuales** e **Informes de configuración**.
Registros de servidores	Permite al usuario administrador asociado al perfil de Management Client ver los registros del sistema, de auditoría y desencadenados por reglas.
Control de acceso	Permite al usuario administrador asociado al perfil de Management Client ver funciones de **Control de acceso**, si ha añadido alguna integración con el sistema de control de acceso o plug-ins a su sistema.

Detalles

En esta sección, decida si un usuario administrador asociado al perfil de Management Client tiene permiso para ver las distintas pestañas para un canal de dispositivos específico, por ejemplo, la pestaña **Ajustes** o **Grabar** para cámaras.

Canal de dispositivos	Descripción
Cámaras	Permite al usuario administrador asociado al perfil de Management Client ver parte o

Canal de dispositivos	Descripción
	la totalidad de los ajustes y las pestañas relacionadas con la cámara.
Micrófonos	Permite al usuario administrador asociado al perfil de Management Client ver la totalidad o parte de los ajustes y las pestañas relacionadas con el micrófono.
Altavoces	Permite al usuario administrador asociado al perfil de Management Client ver la totalidad o parte de los ajustes o las pestañas relacionados con el altavoz.
Metadatos	Permite al usuario administrador asociado al perfil de Management Client ver la totalidad o parte de los ajustes y las pestañas relacionados con los metadatos.
Entrada	Permite al usuario administrador asociado al perfil de Management Client ver la totalidad o parte de los ajustes y las pestañas relacionadas con la entrada.
Salida	Permite al usuario administrador asociado al perfil de Management Client ver la totalidad o parte de los ajustes y las pestañas relacionadas con la salida.

Menú de herramientas

En esta sección, decide si un usuario administrador asociado al perfil de Management Client tiene permiso para ver los elementos que forman parte del menú **Herramientas**.

Opción del menú Herramientas	Descripción
Servicios registrados	Permite al usuario administrador asociado al perfil de Management Client ver **Servicios registrados**.
Cometidos eficaces	Permite al usuario administrador asociado al perfil de Management Client ver **Roles efectivos**.
Opciones	Permite al usuario administrador asociado al perfil de Management Client ver **Opciones**.

Sitios federados

En esta sección, decida si un usuario administrador asociado al perfil de Management Client tiene permiso para ver el panel **Jerarquía de sitios federados**.

Nodo Reglas y eventos

Reglas (nodo Reglas y Eventos)

Su sistema incluye una serie de reglas predeterminadas que puede utilizar para funciones básicas sin configurar nada. Puede desactivar o modificar las reglas predeterminadas según sea necesario. Si modifica o desactiva las reglas predeterminadas, el sistema puede no funcionar según lo deseado ni garantizar que los contenidos de vídeo ni los contenidos de audio se alimentan automáticamente al sistema.

Regla predeterminada	Descripción
Ir a Valor preestablecido cuando PTZ esté hecho	Garantiza que las cámaras PTZ van a sus posiciones preestablecidas respectivas predeterminadas después de haberlas operado manualmente. Este regla no está habilitada de forma predeterminada. Aún cuando haya hagilitado la regla, debe haber definido posiciones preestablecidas predeterminadas para las cámaras PTZ relevantes para que la regla funcione. Esto se hace en la pestaña **Valores preestablecidos**.
Reproducir audio al solicitarlo	Garantiza que el vídeo se graba automáticamente cuando se produce una solicitud externa. La solicitud siempre se desencadena por un sistema que se integra externamente con su sistema, y la regla principalmente la utilizan integradores de sistemas externos o plug-ins.
Grabar en marcador	Garantiza que el vídeo se graba automáticamente cuando un operador establecer un marcador en XProtect Smart Client. Esto se considerando que tenga habilitada la grabación para las cámaras relevantes. La grabación está habilitada de forma predeterminada. El tiempo de grabación predeterminado para esta regla es tres segundos antes de que se establezca el marcados y 30 segundos después de establecer el marcador. Puede editar los tiempos de grabación predeterminados en la regla. El pre-búfer que estableció en la pestaña Grabar debe coincidir con que el tiempo de pregrabación o ser más largo que este.

Regla predeterminada	Descripción
Grabar en movimiento	Garantiza que, siempre que se detecte movimiento en vídeo de cámaras, el vídeo se grabe, siempre que la grabación esté habilitada para las cámaras relevantes. La grabación está habilitada de forma predeterminada. Pese a que la regla predeterminada especifica la grabación basada en la detección de movimiento, esto no garantiza que el sistema grabe vídeo, ya que puede haber deshabilitado grabaciones en cámaras individuales para una o más cámaras. Aún cuando haya habilitado la grabación, recuerde que la calidad de las grabaciones puede verse afectada por ajustes de grabación individuales de la cámara.
Grabar al solicitar	Garantiza que el vídeo se graba automáticamente cuando se produce una solicitud externa, siempre que la grabación esté habilitada para las cámaras relevantes. La grabación está habilitada de forma predeterminada. La solicitud siempre se desencadena por un sistema que se integra externamente con su sistema, y la regla principalmente la utilizan integradores de sistemas externos o plug-ins.
Iniciar contenido de audio	Garantiza que todos los contenidos de audio de todos los micrófonos y altavoces conectados se alimentan automáticamente al sistema. Mientras la regla predeterminada habilita inmediatamente el acceso a contenidos de audio de micrófonos u altavoces conectados tras instalar el sistema, no garantiza que se grabe audio, ya que debe especificar los ajustes de grabación por separado.
Iniciar contenido	Garantiza que los contenidos de vídeo de todas las cámaras conectadas se alimenten automáticamente al sistema. Mientras la regla predeterminada habilita inmediatamente el acceso a contenidos de vídeo de cámaras conectadas tras instalar el sistema, no garantiza que se graben vídeos ya que los ajustes de grabación de las cámaras se deben especificar por separado.
Iniciar contenido de metadatos	Garantiza que los contenidos de datos de todas las cámaras conectadas se alimentan automáticamente al sistema. Mientras la regla predeterminada habilita inmediatamente el acceso a contenidos de datos de cámaras conectadas tras instalar el sistema, no garantiza que se graben datos, ya que los ajustes de grabación de las cámaras se deben especificar

Regla predeterminada	Descripción
	por separado.
Mostrar notificación de solicitud de acceso	Garantiza que todos los eventos de control de acceso categorizados como "Solicitud de acceso", provocarán la aparición de una notificación de solicitud de acceso en XProtect Smart Client, a menos que la función de notificación esté deshabilitada en el perfil de Smart Client.

Recrear reglas predeterminadas

Si accidentalmente elimina alguna de las reglas predeterminadas, puede recrearlas introduciendo el siguiente contenido:

Regla predeterminada	Texto que se debe introducir
Ir al valor preestablecido cuando PTZ esté hecho	Realizar una acción en Sesión manual de PTZ detenida desde Todas las cámaras Mover inmediatamente al valor preestablecido predeterminado en el dispositivo en el que ocurrió el evento
Reproducir audio al solicitarlo	Realizar una acción en Solicitar reproducción de mensaje de audio desde externo Reproducir mensaje de audio desde metadatos en los dispositivos desde metadatos con prioridad 1
Grabar en marcador	Realizar una acción en Referencia de marcador solicitada desde Todas las cámaras, Todos los micrófonos, Todos los altavoces para empezar a grabar tres segundos antes en el dispositivo en el que se produjo el evento Realizar acción 30 segundos después de parar la grabación inmediatamente
Grabar en movimiento	Realizar una acción en Movimiento iniciado desde Todas las cámaras para empezar a grabar tres segundos antes en el dispositivo en el que se produjo el evento Realizar parada de acción en Movimiento detenido desde Todas las cámaras para

Regla predeterminada	Texto que se debe introducir
	parar de grabar tres segundos después
Grabar al solicitar	Realizar una acción en Solicitud e inicio de grabación desde externo para empezar a grabar inmediatamente en los dispositivos desde metadatos Realizar acción de parada en Solicitar parada de grabación desde externo para dejar de grabar inmediatamente
Iniciar contenido de audio	Realizar una acción en un intervalo de tiempo de siempre iniciar el contenido en Todos los micrófonos, Todos los altavoces Realizar una acción, cuando acabe el intervalo de tiempo parar el contenido de inmediato
Iniciar contenido	Realizar una acción en un intervalo de tiempo de siempre iniciar el contenido en Todas las cámaras Realizar una acción, cuando acabe el intervalo de tiempo parar el contenido de inmediato
Iniciar contenido de metadatos	Realizar una acción en un intervalo de tiempo de siempre iniciar el contenido en Todos los metadatos Realizar una acción, cuando acabe el intervalo de tiempo parar el contenido de inmediato
Mostrar notificación de solicitud de acceso	Realizar una acción en Solicitud de acceso (Categorías de control de acceso) desde Sistemas [+ unidades] Mostrar notificación de solicitud de acceso integrado

Perfiles de notificación (nodo Reglas y Eventos)

Especifique las siguientes propiedades para los perfiles de notificación:

Componente	Requisito
Nombre	Introduzca 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)	Introduzca una descripción del perfil de notificación. La descripción aparece cuando se pausa el puntero del ratón sobre el perfil de notificación en la lista **Perfiles de notificación** del panel Descripción general.
Destinatarios	Introduzca las direcciones de correo electrónico a las que se deben enviar las notificaciones de correo electrónico del perfil de notificación. Para introducir más de una dirección de correo electrónico, separe las direcciones con punto y coma. Ejemplo: aa@aaaa.aa;bb@bbbb.bb;cc@cccc.cc
Asunto	Introduzca el texto que quiere que aparezca como asunto de la notificación de correo electrónico. Puede insertar variables del sistema, como **Nombre del dispositivo**, en el campo del texto del mensaje. Para insertar variables, haga clic en los enlaces de variables requeridos en la casilla debajo del campo.
Texto del mensaje	Introduzca el texto que quiere que aparezca en el cuerpo de las notificaciones de correo electrónico. Además del texto del mensaje, el cuerpo de cada notificación de correo electrónico contiene automáticamente esta información: • Qué desencadenó la notificación de correo electrónico • La fuente de cualquier imagen fija o videoclip AVI adjuntados
Tiempo entre correos electrónicos	Especifique el tiempo mínimo requerido (en segundos) que deben pasar entre el envío de cada notificación de correo electrónico. Ejemplos: • Si especifica un valor de **120**, transcurre un mínimo de 2 minutos entre el envío de cada notificación de correo electrónico, incluso si el perfil de notificación se vuelve a desencadenar por una regla antes de que hayan transcurrido 2 minutos

Componente	Requisito
	• Si especifica un valor de **0**, las notificaciones de correo electrónico se envían cada vez que una regla desencadene el perfil de notificación. Esto puede potencialmente provocar el envío de un gran número de notificaciones de correo electrónico. Si utiliza el valor **0**, debe, por tanto, considerar con detenimiento si quiere usar el perfil de notificación en reglas que es probable que se desencadene con frecuencia
Número de imágenes	Especifique el número máximo de imágene fiijas que quiere incluir en cada una de las notificaciones de correo electrónico del perfil de notificación. El valor predeterminado es cinco imágenes.
Tiempo entre imágenes (ms)	Especifique el número de milisegundos que quiere entre las grabaciones presentadas en las imágenes incluidas. Ejemplo: Con el valor predeterminado de 500 milisegundos, las imágenes incluidas muestran grabaciones con medio segundo entre ellas.
Tiempo antes del evento (segundos)	Este ajuste se utiliza para especificar el inicio del archivo AVI. De forma predeterminada, el archivo AVI contiene grabaciones de 2 segundos antes de que se desencadene el pefil de notificación. Puede cambiar esto en el número de segundos que requiere.
Tiempo después del evento (segundos)	Este ajuste se utiliza para especificar el final del archivo AVI. De forma predeterminada, el archivo AVI termina 4 segundos después de que se desencadene el perfil de notificación. Puede cambiar esto en el número de segundos que requiere.
Velocidad de fotogramas	Especifique el número de fotogramas por segundo que quiere que contenga el archivo AVI. El valor predeterminado es cinco fotogramas por segundo. Cuanto mayor sea la velocidad de los fotogramas, mayor será la calidad de la imagen y el tamaño del archivo AVI.
Incrustar imágenes en correo electrónico	Si se selecciona (predeeterminado), las imágenes se insertan en el cuerpo de las notificaciones de correo electrónico. Si no, las imágenes se incluyen en notificaciones de correo electrónico como archivos adjuntos.

Descripción general de eventos

Al añadir una regla basada en eventos en el asistente **Gestionar regla**, puede seleccionar entre una serie de tipos de evnto distintos. Para obtener una buena descripción general, los eventos que puede seleccionar están recogidos en grupos en función de si son:

Hardware:

Algún hardware puede crear eventos por sí mismo, por ejemplo, para detectar movimiento. Puede utilizar estos como eventos, pero debe configurarlos en el hardware antes de poder usarlos en el sistema. Puede que solo sea capaz de utilizar los eventos enumerados en parte del hardware, ya que no todos los tipos de cámaras pueden detectar alteraciones o cambios de temperatura.

Hardware - Eventos configurables:

Los eventos configurables de hardware se importan de forma automática desde controladores de dispositivos. Esto significa que varían según el hardware y no se documentan aquí. Los eventos configurables no se desencadenan hasta que los ha añadido al sistema y los ha configurado en la pestaña **Evento** para hardware. Algunos de los eventos configurables también requieren que configure la propia cámara (hardware).

Hardware - Eventos predefinidos:

Evento	Descripción
Error de comunicación (hardware)	Se produce cuando se pierde una conexión con el hardware.
Comunicación iniciada (hardware)	Se produce cuando se establece con éxito la comunicación con el hardware.
Comunicación detenida (hardware)	Se produce cuando se detiene con éxito la comunicación con el hardware.

Dispositivos - Eventos configurables:

Los eventos configurables de dispositivos se importan de forma automática desde controladores de dispositivos. Esto quiere decir que varían de un dispositivo a otro y no se documentan aquí. Los eventos configurables no se desencadenan hasta que los ha añadido al sistema y los ha configurado en la pestaña **Evento** en un dispositivo.

Dispositivos - Eventos predefinidos:

Evento	Descripción
Referencia de marcador solicitada	Se produce cuando se crea un marcador en directo en los clientes. Asimismo, un requisito para usar el registro predeterminado en la regla de marcadores.
Error de comunicación (Dispositivo)	Se produce cuando se pierde una conexión con 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 comunicación con un dispositivo.
Comunicación detenida (Dispositivo)	Se produce cuando se detiene con éxito la comunicación con un dispositivo.
Bloqueo de evidencias cambiado	Se produce cuando un bloqueo de evidencias para dispositivos lo cambia un usuario cliente o cuando se cambia mediante MIP SDK.
Evidencia bloqueada	Se produce cuando un bloqueo de evidencias para dispositivos lo crea un usuario cliente o cuando se crea mediante MIP SDK.
Evidencia desbloqueada	Se produce cuando un bloqueo de evidencias para dispositivos lo quita un usuario cliente o cuando se quita mediante MIP SDK.
Desbordamiento de entrada iniciado	El desbordamiento de contenido (desbordamiento de medios) se produce cuando un servidor de grabación no puede procesar los datos recibidos tan rápido como está especificado en la configuración y, por tanto, se ve forzado a descartar algunas grabaciones. Si el servidor está en buenas condiciones, normalmente se produce un desbordamiento de contenido como consecuencia de una escritura lenta en el disco. Puede solucionar esto reduciendo la cantidad de datos escritos o mejorando el rendimiento del almacenamiento del sistema. Reduzca la cantidad de datos escritos reduciendo las velocidades de fotogramas, la resolución o la

Evento	Descripción
	calidad de la imagen en sus cámaras, pero esto puede degradar la calidad de las grabaciones. Si no está interesado en eso, en lugar de mejorar el rendimiento de su sistema de almacenamiento instalando unidades adicionales para compartir la carga o instalando controladores o discos más rápidos. Puede utilizar este evento para desencadenar acciones que ayuden a evitar el problema, por ejemplo, para reducir la velocidad de grabación de fotogramas.
Desbordamiento de entrada detenido	Se produce cuando termina un desbordamiento de contenido (consulte Desbordamiento de entrada iniciado en la página 505).
Entrada de cliente en directo solicitada	Se produce cuando los usuarios clientes solicitan una transmisión en directo desde un dispositivo. El evento se produce en el momento de la solicitud, incluso si la solicitud del usuario cliente resulta posteriormente infructuosa, por ejemplo, porque el usuario cliente no tiene los permisos necesarios para ver la transmisión en directo solicitada o porque la transmisión se ha detenido por algún motivo.
Entrada de cliente en directo terminada	Se produce cuando los usuarios clientes ya no solicitan una transmisión en directo desde un dispositivo.
Grabación manual iniciada	Se produce cuando un usuario cliente empieza 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 detiene una sesión de grabación para una cámara. Si el sistema de reglas también ha iniciado una sesión de grabación, continúa grabando incluso después de que se detenga la grabación manual.
Referencia de datos marcados solicitada	Se produce cuando un bloqueo de evidencias se realiza en modo de reproducción en los clientes o mediante MIP SDK. Se crea un evento que puede usar en sus reglas.
Movimiento	Se produce cuando el sistema detecta movimiento en vídeo recibido de cámaras.

Evento	Descripción
iniciado	Este tipo de evento requiere que la detección de movimiento del sistema esté habilitada para las cámaras as las que está vinculado el evento. Además de la detección de movimiento del sistema, algunas cámaras pueden detectar movimiento por sí solas y desencadenar el evento de **Movimiento iniciado (HW)**, pero depende de la configuración del hardware de la cámara y del sistema. Consulte también Hardware - Eventos configurables: en la página 504.
Movimiento detenido	Se produce cuando deja de detectarse movimiento en el vídeo recibido. Consulte también Movimiento iniciado en la página 506. Este tipo de evento requiere que la detección de movimiento del sistema esté habilitada para las cámaras as las que está vinculado el evento. Además de la detección de movimiento del sistema, algunas cámaras pueden detectar movimiento por sí mismas y desencadenar el evento Movimiento detenido (HW), pero depende de la configuración del hardware de la cámara y del sistema. Consulte también Hardware - Eventos configurables: en la página 504.
Salida activada	Se produce cuando se activa un puerto de salida externo en un dispositivo. Este tipo de evento requiere que al manos un dispositivo de su sistema admita puertos de salida.
Salida cambiada	Se produce cuando se cambia el estado de un puerto de salida externo en un dispositivo. Este tipo de evento requiere que al manos un dispositivo de su sistema admita puertos de salida.
Salida desactivada	Se produce cuando se desactiva un puerto de salida externo en un dispositivo. Este tipo de evento requiere que al manos un dispositivo de su sistema admita puertos de salida.
Sesión manual de PTZ iniciada	Se produce cuando se inicia una sesión de PTZ operada manualmente (en oposición a una sesión de PTZ basada en vigilancia programada o desencadenada automáticamente por un evento) en una cámara. Este tipo de evento requiere que las cámaras a las que está vinculado este evento sean cámaras PTZ.

Evento	Descripción
Sesión manual de PTZ detenida	Se produce cuando se detiene una sesión de PTZ operada manualmente (en oposición a una sesión de PTZ basada en vigilancia programada o desencadenada automáticamente por un evento) en una cámara. Este tipo de evento requiere que las cámaras a las que está vinculado este evento sean cámaras PTZ.
Grabación iniciada	Se produce cada vez que se inicia una grabación. Existe un evento separado para la grabación manual iniciada.
Grabación detenida	Se produce cada vez que se detiene una grabación. Hay un evento separado para la grabación manual detenida.
Configuración cambiada	Se produce cuando los ajustes en un dispositivo se cambian correctamente.
Error de cambio de configuración	Se produce cuando se hace un intento de cambiar los ajustes en un dispositivo, y el intento no tiene éxito.

Eventos externos - Eventos predefinidos:

Evento	Descripción
Solicitar la reproducción de mensajes de audio	Se activa cuando se solicitan mensajes de reproducción de audio mediante el MIP SDK. Mediante el MIP SDK un tercer proveedor puede desarrollar plug-ins personalizados (por ejemplo, integración con sistemas de control de acceso externos o similar) para su sistemas.
Solicitar inicio de grabación	Se activa cuando se solicita iniciar grabaciones mediante el MIP SDK. Mediante el MIP SDK un tercer proveedor puede desarrollar plug-ins personalizados (por ejemplo, integración con sistemas de control de acceso externos o similar) para su sistemas.
Solicitar parada de	Se activa cuando se solicita parar grabaciones mediante el MIP SDK.

Evento	Descripción
grabación	Por medio de MIP SDK un proveedor tercero puede desarrollar plug-ins personalizados (por ejemplo, integración con sistemas de control de acceso o similar) para su sistema.

Eventos externos - Eventos genéricos:

Los eventos genéricos le permiten desencadenar acciones en el sistema enviando cadenas sencillas mediante la red IP al sistema. La finalidad de los eventos genéricos es permitir que tantas fuentes externas como sea posible interactúen con el sistema.

Eventos externos - Eventos definidos por el usuario:

También puede seleccionar una serie de eventos personalizados para adaptarse a su sistema. Puede utilizar estos eventos definidos por el usuario para:

- Permitiendo a los usuarios de clientes desencadenar manualmente eventos mientras visualiza vídeo en directo en los clientes
- Incontables fines adicionales. Por ejemplo, puede crear eventos definidos por el usuario que ocurren si se recibe un un tipo concreto de un dispositivo

  Consulte también Eventos definidos por el usuario (explicación) en la página 83.

Servidores de grabación:

Evento	Descripción
Archivo disponible	Se produce cuando un archivo para un servidor de grabaciones pasa estar disponible después de de haber estado no disponible. Consulte también Archivo no disponible en la página 509.
Archivo no disponible	Se produce cuando un archivo para un servidor de grabaciones pasa a no estar disponible, por ejemplo, si se pierde la conexión con un archivo ubicado en una unidad de red. En esos casos, no puede archivar grabaciones. Puede utilizar el evento para, por ejemplo, desencadenar una alarma o un perfil de notificación para que se envíe automáticamente una notificación de correo electrónico a las personas relevantes de su organización.

Evento	Descripción
Archivo no terminado	Se produce cuando un archivo para un servidor de grabaciones no ha terminado con la última ronda de archivado cuando la siguiente está programada para empezar.
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 del tamaño de la base de datos antes del límite de tiempo de retención.
Disco de la base de datos lleno: archivado automático	Se produce cuando un disco de la base de datos está lleno. Un disco de la base de datos está lleno cuando quedan menos de 5 GB de espacio en el disco: Los datos más antiguos de una base de datos siempre se archivan de forma automática (o se eliminan si no se ha definido el siguiente archivo) cuando hay menos de 5 GB de espacio libre.
Disco de base de datos lleno - Eliminando	Se produce cuando un disco de la base de datos está lleno y queda menos de 1 GB libre. Los datos se seleccionan incluso si se define un siguiente archivo. Una base de datos siempre requiere 250 MB de espacio libre. Si se alcanza este límite (si los datos no se eliminan lo bastante rápido), no se escriben más datos en la base de datos hasta qye se haya liberado espacio suficiente. El tamaño máximo real de su base de datos es el número de gigabytes que especifique, menos 5 GB.
Base de datos llena: autoarchivado	Se produce cuando un archivo para un servidor de grabaciones está lleno y necesita autoarchivar en un archivo en el almacenamiento.
Reparación de base de datos	Se produce si una base de datos queda dañada, en cuyo caso el sistema intenta automáticamente dos métodos distintos para reparar bases de datos: una reparación rápida y una reparación pormenorizada.
Área de	Se produce cuando un almacenamiento para un servidor de grabaciones pasa a

Evento	Descripción
almacenamiento disponible	estar disponible después de haber estado no disponible. Consulte también Almacenamiento de base de datos no disponible en la página 511. Puede, por ejemplo, utilizar el evento para empezar a grabar si se ha parado por un evento de **Almacenamiento de base datos no disponible**.
Almacenamiento de base de datos no disponible	Se produce cuando un almacenamiento para un servidor de grabaciones pasa a no estar disponible, por ejemplo, si se pierde la conexión con el almacenamiento ubicado en la unidad de red. En esos casos, no puede archivar grabaciones. Puede utilizar el evento para, por ejemplo, parar de grabar, desencadenar una alarma o un perfil de notificación para que se envíe automáticamente una notificación de correo electrónico a las personas relevantes de su organización.
Error de comunicación cifrada failover	Se produce cuando hay un error de comunicación SSL entre el servidor de failover y los servidores de grabación monitorizados.
Failover iniciado	Se produce cuando un servidor de grabaciones de failover asume el control de un servidor de grabación. Consulte también Servidores de failover (nodo).
Failover detenido	Se produce cuando un servidor de grabación vuelve a estar disponible y puede asumir el control de un servidor de grabación failover.

Eventos del monitor del sistema

Los eventos del monitor del sistema se desencadenan mediante valores de umbrales superados configurados en el nodo **Umbrales del monitor del sistema**. Consulte también Ver el estado actual de su hardware y solucionar problema en caso necesario en la página 302.

Esta funcionalidad requiere que el servicio Data Collector esté en ejecución.

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 advertencia de la CPU.
Aviso de uso de CPU	Se produce cuando el uso de la CPU excede el umbral de advertencia de la CPU o cae por debajo del umbral crítico de la CPU.
Uso de memoria crítico	Se produce cuando el uso de memoria excede el umbral crítico de memoria.
Uso de memoria normal	Se produce cuando el uso de memoria cae por debajo del umbral de advertencia de memoria.
Aviso de uso de memoria	Se produce cuando el uso de memoria excede el umbral de advertencia de memoria o cae por debajo del umbral crítico de uso de memoria.
Decodificación de NVIDIA crucial	Se produce cuando el uso de decodificación de NVIDIA excede el umbral de decodificación crítico de NVIDIA.
Decodificación de NVIDIA normal	Se produce cuando el el uso de decodificación de NVIDIA cae por debajo del umbral de advertencia de decodificación de NVIDIA.
Aviso de la decodificación de NVIDIA	Se produce cuando el uso de decodificación de NVIDIA excede el umbral de advertencia de decodificación de NVIDIA o cae por debajo del umbral crítico de decodificación de NVIDIA.
Memoria de NVIDIA crucial	Se produce cuando el uso de memoria de NVIDIA excede el umbral crítico de memoria de NVIDIA.
Memoria de NVIDIA normal	Se produce cuando el uso de memoria de NVIDIA cae por debajo del umbral de advertencia de memoria de NVIDIA.
Aviso de la memoria de NVIDIA	Se produce cuando el uso de memoria de NVIDIA excede el umbral de advertencia de memoria de NVIDIA o cae por debajo del umbral crítico de

Evento	Descripción
	memoria de NVIDIA.
Procesamiento de NVIDIA crucial	Se produce cuando el uso de renderización de NVIDIA excede el umbral crítico de renderización de NVIDIA.
NVIDIA normal de representación	Se produce cuando el uso de renderización de NVIDIA cae por debajo del umbral de advertencia de renderización de NVIDIA.
Aviso del procesamiento de NVIDIA	Se produce cuando el uso de renderización de NVIDIA excede el umbral de advertencia de renderización de NVIDIA o cae por debajo del umbral crítico de renderización de NVIDIA.
Servicios disponibles crítico	Se produce cuando un servicio de servidor deja de ejecutarse. No hay valores de umbrales para este evento.
Servicios disponibles normal	Se produce cuando un estado del servicio del servidor cambia a en ejecución. No hay valores de umbrales para este evento.

Monitor del sistema - Cámara:

Evento	Descripción
FPS en directo crítico	Se produce cuando la tasa de FPS en directo cae por debajo del umbral crítico de FPS en directo.
FPS en directo normal	Se produce cuando una tasa de FPS en directo excede el umbral de advertencia de FPS en directo.
Aviso de FPS en directo	Se produce cuando la tasa de FPS en directo cae por debajo del umbral de advertencia de FPS en directo o excede el umbral crítico de FPS en directo.
Grabando FPS crítico	Se produce cuando la tasa de FPS de grabación cae por debajo del umbral crítico de FPS de grabación.

Evento	Descripción
Grabando FPS normal	Se produce cuando la tasa de FPS de grabación excede el umbral de advertencia de FPS de grabación.
Aviso de grabando FPS	Se produce cuando la tasa de FPS de grabación cae por debajo del umbral de advertencia de FPS de grabación o excede el umbral crítico de FPS de grabación.
Espacio utilizado crítico	Se produce cuando el almacenamiento utilizado para grabaciones por una cámara concreta excede el umbral crítico de espacio utilizado.
Espacio utilizado normal	Se produce cuando el almacenamiento utilizado para grabaciones por una cámara concreta cae por debajo del umbral de advertencia de espacio utilizado.
Aviso de espacio utilizado	Se produce cuando el almacenamiento utilizado para grabaciones por una cámara concreta excede el umbral de advertencia de espacio utilizado o cae por debajo del umbral crítico de espacio utilizado.

Monitor del sistema - Disco:

Evento	Descripción
Espacio libre crítico	Se produce cuando el uso del espacio en el disco excede el umbral crítico de espacio libre.
Espacio libre normal	Se produce cuando el uso de espacio en el disco cae por debajo del umbral de advertencia de espacio libre.
Aviso de espacio libre	Se produce cuando el uso del espacio en el disco excede el umbral de advertencia de espacio libre o cae por debajo del umbral crítico de espacio libre.

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 del umbral crítico de tiempo de retención. Por ejemplo, cuando los datos de flujos de vídeo están llenando el almacenamiento más rápido de lo esperado.
Periodo de retención normal	Se produce cuando el sistema predice que el almacenamiento se llenará más lento que el valor del umbral de advertencia del tiempo de retención. Por ejemplo, cuando loa datos de los flujos de vídeo están llenando 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 que el valor del umbral de advertencia del tiempo de retención o más lento que el valor del umbral crítico del tiempo de retención. Por ejemplo, cuando los datos de flujos de datos están llenando el almacenamiento más rápido de lo esperado debido a la detección de más movimiento por las cámaras configuradas para grabar al detectar movimiento.

Otro:

Evento	Descripción
Error en la activación automática de licencia	Se produce cuando falla la activación de la licencia automática en línea. No hay valores umbrales para este evento.
Cambio de contraseña programado iniciado	Se produce cuando comienza un cambio de contraseña programado.
Cambio de contraseña programado completado con éxito	Se produce cuando un cambio de contraseña programado se completa sin errores.
Cambio de contraseña programado completado con errores	Se produce cuando un cambio de contraseña programado se completa con errores.

Eventos de productos e integraciones adicionales:

Los eventos de productos e integraciones adicionales se pueden usar en el sistema de reglas, por ejemplo:

- Los eventos de análisis también se pueden usar en el sistema de reglas

Acciones y acciones de parada

Hay un conjunto de acciones y acciones de parada disponibles para la creación de reglas en el asistente de **Gestionar regla**. Puede tener más acciones disponibles si la instalación de su sistema utiliza productos complementarios o plug-ins específicos del proveedor. Para cada tipo de acción, se recoge la información de la acción de parada en caso de ser relevante.

Asistente de gestión de reglas

Acción	Descripción
Iniciar grabación en <dispositivos>	Inicie la grabación y el guardado de los datos en la base de datos desde los dispositivos seleccionados. Al seleccionar este tipo de acción, el asistente **Gestionar regla** le pide que especifique: Cuándo debe empezar la grabación. Esto ocurre inmediatamente o unos segundos antes del desencadenamiento del evento/comienzo del intevalo de tiempo de desencadenamiento y en qué dispositivos debe tener lugar la acción. Este tipo de acción requiere que haya habilitado la grabación en los dispositivos a los que está vinculada la acción. Solo puede guardar datos de antes de un evento o un intervalo de tiempo si ha habilitado el almacenamiento previo en búfer para los dispositivos relevantes. Habilite la grabación y especifique los ajustes de almacenamiento previo en búfer para un dispositivo en la pestaña **Grabar**. **Acción de parada requerida**: Este tipo de acción requiere una o más acciones de parada. En uno de los siguientes pasos, el asistente le pide automáticamente que especifique la acción de parada: **Parar grabación**. Sin esta acción de parada, la grabación potencialmente continuaría de manera indefinida. También tiene la opción de especificar más acciones de parada.

Acción	Descripción
Iniciar directo en <dispositivos>	Comience la alimentación de contenido desde dispositivos al sistema. Al iniciar la alimentación de contenido desde un dispositivo, los datos se transfieren del dispositivo al sistema, en cuyo caso puede ver y grabar, dependiendo del tipo de datos. Al seleccionar este tipo de acción, el asistente **Gestionar regla** le pide que especifique en qué dispositivos iniciar el envío de contenido. El sistema incluye una regla predeterminada que garantiza que los contenidos siempre se inicien en todas las cámaras. **Acción de parada requerida**: Este tipo de acción requiere una o más acciones de parada. En uno de los siguientes pasos, el asistente le pide automáticamente que especifique la acción de parada: **Parar contenido**. También puede especificar más acciones de parada. Utilizar la acción de parada obligatoria **Parar contenido** para parar el contenido de un dispositivo significa que los datos dejan de transferirse desde el dispositivo al sistema, en cuyo caso la visualización y la grabación de vídeo en directo, por ejemplo, ya no es posible. Sin embargo, un dispositivo en el que ha detenido la alimentación de fuentes puede seguir comunicándose con el servidor de grabaciones, y puede volver a comenzar la alimentación de contenido, en contraposición a cuando se ha deshabilitado manualmente el dispositivo.  Pese a que este tipo de acción habilita el acceso a contenidos de datos de dispositivos seleccionados, no garantiza que los datos se graben, ya que debe especificar los ajustes de grabación por separado.
Ajustar <Smart Wall> para el <valor preestablecido>	Establece XProtect Smart Wall en un ajuste predefinido seleccionado. Especifique el valor preestablecido en la pestaña **Valores preestablecidos de Smart Wall**. **Ninguna acción de detención obligatoria**: Este tipo de acción no requiere una acción de detención.Puede especificar acciones de parada opcionales que se deben llevar a cabo en un evento o después de un periodo de tiempo.

Acción	Descripción
Ajustar <monitor> de <Smart Wall> para mostrar <cámaras>	Establece un monitor de XProtect Smart Wall específico para mostrar vídeo en directo de las cámaras seleccionadas en este sitio o en cualquier sitio secundario configurado en Milestone Federated Architecture. **Ninguna acción de detención obligatoria**: Este tipo de acción no requiere una acción de detención.Puede especificar acciones de parada opcionales que se deben llevar a cabo en un evento o después de un periodo de tiempo.
Establecer <Smart Wall> <monitor> para mostrar texto <mensajes>	Establece un monitor de XProtect Smart Wall específico para mostrar un mensaje de texto definido por el usuario de un máximo de 200 caracteres. **Ninguna acción de detención obligatoria**: Este tipo de acción no requiere una acción de detención.Puede especificar acciones de parada opcionales que se deben llevar a cabo en un evento o después de un periodo de tiempo.
Eliminar <cameras> del monitor <Smart Wall> <monitor>	Deje de mostrar vídeo de una cámara específica. **Ninguna acción de detención obligatoria**: Este tipo de acción no requiere una acción de detención.Puede especificar acciones de parada opcionales que se deben llevar a cabo en un evento o después de un periodo de tiempo.
Ajustar velocidad de fotogramas de directo a <dispositivos>	Establece una velocidad de fotogramas concreta para usar cuando el sistema muestra vídeo en directo de las cámaras seleccionadas que substituye a la velocidad de fotogramas predeterminada de la cámara. Especifique esto en la pestaña **Ajustes**. Al seleccionar este tipo de acción, el asistente **Gestionar regla** le pide que especifique qué velocidad de fotogramas establecer y en qué dispositivos. Verifique siempre que la velocidad de fotogramas que especifique esté disponible en las cámaras relevantes. **Acción de parada requerida**: Este tipo de acción requiere una o más acciones de parada. En uno de los siguientes pasos, el asistente le pide automáticamente que especifique la acción de parada: **Retaurar velocidad de fotogramas en directo predeterminada**. Sin esta acción de parada, la velocidad de fotogramas

Acción	Descripción
	predeterminada potencialmente no se restablecería nunca. También tiene la opción de especificar más acciones de parada.
Ajustar velocidad de fotogramas de grabación en <dispositivos>	Establece una velocidad de fotogramas concreta para usar cuando el sistema guarda vídeo grabado de las cámaras seleccionadas en la base de datos, en lugar de la velocidad de fotogramas de grabación predeterminada de la cámara. Al seleccionar este tipo de acción, el asistente **Gestionar regla** le pide que especifique qué velocidad de fotogramas establecer y en qué cámaras. Solo puede especificar una velocidad de grabación de fotogramas para JPEG, un codificador de vídeo con el que cada fotograma se comprime por separado en una imagen JPEG. Este tipo de acción también requiere que haya habilitado la grabación en las cámaras con las que está vinculada la acción. Habilite la grabación para una cámara en la pestaña **Grabar**. La máxima velocidad de fotogramas que puede especificar depende de los tipos relevantes de cámara y de su resolución de imagen seleccionada. **Acción de parada requerida**: Este tipo de acción requiere una o más acciones de parada. En uno de los siguientes pasos, el asistente le pide automáticamente que especifique la acción de parada: **Restaure la velocidad de grabación de fotogramas predeterminada**. Sin esta acción de parada, la velocidad de grabación de fotogramas potencialmente no se restablecería nunca. También tiene la opción de especificar más acciones de parada.
Ajustar velocidad de grabación de fotogramas en todos los fotogramas para MPEG-4/H.264/H.265 en <dispositivos>	Establece la velocidad de fotogramas para grabar todos los fotogramas cuando el sistema guarda vídeo grabado de las cámaras seleccionadas en la base de datos, en lugar de solo fotogramas clave. Habilite la función de grabación solo de fotogramas clave en la pestaña **Grabar**. Cuando selecciona este tipo de acción, el asistente **Gestionar regla** le pide que seleccione qué dispositivos a los que debe aplicarse esta acción. Solo puede habilitar la grabación de fotogramas clave para MPEG-

Acción	Descripción
	4/H.264/H.265. Este tipo de acción también requiere que tenga habilitada la grabación en las cámaras a las que está vinculada la acción. Habilite la grabación para una cámara en la pestaña **Grabar**. **Acción de parada requerida**: Este tipo de acción requiere una o más acciones de parada. En uno de los pasos siguientes, el asistente le pide automáticamente que especifique la acción de parada: **Restaurar velocidad de fotogramas clave predeterminada de grabación para MPEG-4/H.264/H.265** Sin esta acción de parada, el ajuste predeterminado potencialmente no se restablecería nunca. También tiene la opción de especificar más acciones de parada.
Iniciar vigilancia en <dispositivo> utilizando <perfil> con prioridad de PTZ <prioridad>	Empieza la vigilancia de PTZ de acuerdo con un perfil de vigilancia concreto para una cámara PTZ concreta con una prioridad concreta. Esta es una definición exacta de cómo se debe llevar a cabo la la vigilancia, incluida la secuencia de posiciones predefinidas, los ajustes de temporización y más. Si ha actualizado su sistema desde una versión anterior del sistema, los valores antiguo (**Muy bajo**, **Bajo**, **Medio**, **Alto** y **Muy alto**) se han traducido del siguiente modo: • Muy bajo = 1000 • Bajo = 2000 • Medio = 3000 • Alto = 4000 • Muy alto = 5000 Al seleccionar este tipo de acción, el asistente **Gestionar regla** le pide que seleccione un perfil de vigilancia. Solo puede seleccionar un perfil de vigilancia en un dispositivo y no puede seleccionar varios perfiles de vigilancia. Este tipo de acción requiere que los dispositivos a los que está vinculada sean dispositivos PTZ.

Acción	Descripción
	Debe definir al menos un perfil de vigilancia para el/los dispositivo(s). Puede definir perfiles de vigilancia para una cámara PTZ en la pestaña **Vigilancia**. **Acción de parada requerida**: Este tipo de acción requiere una o más acciones de parada. En uno de los pasos siguientes, el asistente le pide automáticamente que especifique la acción de parada: **Detener patrulla** Sin esta acción de parada, la vigilancia potencialmente no pararía nunca. También puede especificar más acciones de parada.
Detener patrulla en <dispositivos>	Pausa la vigilancia de PTZ. Al seleccionar este tipo de acción, el asistente **Gestionar regla** le pide que especifique los dispositivos en los que pausar la vigilancia. Este tipo de acción requiere que los dispositivos a los que está vinculada sean dispositivos PTZ. Debe definir al menos un perfil de vigilancia para el/los dispositivo(s). Puede definir perfiles de vigilancia para una cámara PTZ en la pestaña **Vigilancia**. **Acción de parada requerida**: Este tipo de acción requiere una o más acciones de parada. En uno de los siguientes pasos, el asistente le pide automáticamente que especifique la acción de parada: **Reanudar patrulla** Sin esta acción de parada, la vigilancia potencialmente se pausaría de manera indefinida. También tiene la opción de especificar más acciones de parada.

Acción	Descripción
Mover <dispositivo> a posición <preestablecida> con prioridad de PTZ <prioridad>	Mueve una cámara concreta a una posición preestablecida concreta - sin embargo, siempre de acuerdo con la prioridad. Al seleccionar este tipo de acción, el asistente **Gestionar regla** le pide que seleccione una posición predefinida. Solo se puede seleccionar una posición predefinida en una cámara. No es posible seleccionar varias posiciones predefinidas. Este tipo de acción requiere que los dispositivos a los que está vinculada sean dispositivos PTZ. Esta acción requiere que haya definido al menos una posición predefinida para estos dispositivos. Define posiciones preestablecidas para una cámara PTZ en la pestaña **Valores preestablecidos**. **Ninguna acción de detención obligatoria**: Este tipo de acción no requiere una acción de detención.Puede especificar acciones de parada opcionales que se deben llevar a cabo en un evento o después de un periodo de tiempo.
Mover a valor preestablecido predeterminado en <dispositivos> con prioridad de PTZ <prioridad>	Mueve una o más cámaras concretas a sus posiciones preestablecidas predeterminadas respectivas - sin embargo, siempre de acuerdo con la prioridad. Cuando selecciona este tipo de acción, el asistente **Gestionar regla** le pide que seleccione qué dispositivos a los que debe aplicarse esta acción.

Acción	Descripción
	Este tipo de acción requiere que los dispositivos a los que está vinculada sean dispositivos PTZ. Esta acción requiere que haya definido al menos una posición predefinida para estos dispositivos. Define posiciones preestablecidas para una cámara PTZ en la pestaña **Valores preestablecidos**. **Ninguna acción de detención obligatoria**: Este tipo de acción no requiere una acción de detención.Puede especificar acciones de parada opcionales que se deben llevar a cabo en un evento o después de un periodo de tiempo.
Ajustar salida de dispositivo a <estado>	Establece una salida en un dispositivo a un estado concreto (activado o desactivado). Al seleccionar 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 está vinculada la acción tengan cada uno al menos una unidad de salida externa conectada a un puerto de salida. **Ninguna acción de detención obligatoria**: Este tipo de acción no requiere una acción de detención.Puede especificar acciones de parada opcionales que se deben llevar a cabo en un evento o después de un periodo de tiempo.
Crear marcador en <dispositivo>	Crea un marcador en flujos en directo o grabaciones de un dispositivo seleccionado. Un favorito facilita hacer un seguimiento de un cierto evento o periodo en el 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 de marcadores y que seleccione dispositivos. **Ninguna acción de detención obligatoria**: Este tipo de acción no requiere una acción de detención.Puede especificar acciones de parada opcionales que se deben llevar a cabo en un evento o después de un periodo de tiempo.

Acción	Descripción
Reproducir <message> de audio en <devices> con <priority>	Reproduzca un mensaje de audio en dispositivos seleccionados desencadenado por un evento. Los dispositivos son principalmente altavoces o cámaras. Este tipo de acción requiere que haya cargado el mensaje en el sistema en la pestaña **Herramientas** > **Opciones** > **Mensajes de audio**. Puede crear más reglas para el mismo evento y enviar distintos mensajes a cada dispositivo, pero siempre según la prioridad. Las propiedades que controlan la secuencia son aquellas establecidas en la regla y en el dispositivo para un rol en la pestaña **Habla**: • Si se reproduce un mensaje y se envía otro mensaje con la misma priodidad al mismo altavoz, el primer mensaje se completará y luego empieza el segundo • Si se reproduce un mensaje y se envía otro mensaje con una prioridad más alta al mismo altavoz, el primer mensaje se interrumpe y el segundo comienza de inmediato
Enviar notificación a <perfil>	Envía una notificación utilizando un perfil de notificación concreto. Al seleccionar este tipo de acción, el asistente **Gestiona regla** le pide que seleccione un perfil de notificación y de qué dispositivos incluir imágenes previas a la alarma. Solo puede seleccionar un perfil de notificación y no puede seleccionar varios perfiles de notificación. Un único perfil de notificación puede contener varios destinatarios. También puede crear más reglas para el mismo evento y enviar distintas notificaciones a cada uno de los perfiles de notificación. Puede copiar y reutilizar el contenido de las reglas haciendo clic con el botón derecho en una regla en la lista **Reglas**. Este tipo de acción requiere que haya definido al menos un perfil de notificaciones. Las imágenes previas a la alarma solo se incluyen si ha habilitado la opción **Incluir imágenes** para el perfil de notificación relevante. **Ninguna acción de detención obligatoria**: Este tipo de acción no requiere una acción de detención.Puede especificar acciones de parada opcionales que se deben llevar a cabo en un evento o después de un periodo de tiempo.

Acción	Descripción
Crear nueva <entrada de registro>	Genera una entrada en el registro de reglas. Al seleccionar este tipo de acción, el asistente **Gestionar regla** le pide que especifique un texto para la entrada de registro. Al especificar el texto del registro, puede insertar variables, como **$DeviceName$** y **$EventName$** en el mensaje del registro. **Ninguna acción de detención obligatoria**: Este tipo de acción no requiere una acción de detención.Puede especificar acciones de parada opcionales que se deben llevar a cabo en un evento o después de un periodo de tiempo.
Iniciar plug-in en <dispositivos>	Inicia uno o más plug-ins. Al seleccionar este tipo de acción, el asistente **Gestionar regla** le pide que seleccione plug-ins requeridos y en qué dispositivos iniciar los plug-ins. Este tipo de acción requiere que tenga al menos uno o más plug-ins instalados en su sistema. **Ninguna acción de detención obligatoria**: Este tipo de acción no requiere una acción de detención.Puede especificar acciones de parada opcionales que se deben llevar a cabo en un evento o después de un periodo de tiempo.
Detener plug-in en <dispositivos>	Para uno o más plug-ins. Al seleccionar este tipo de acción, el asistente **Gestionar regla** le pide que seleccione los plug-ins requeridos y en qué dispositivos detener los plug-ins. Este tipo de acción requiere que tenga al menos uno o más plug-ins instalados en su sistema. **Ninguna acción de detención obligatoria**: Este tipo de acción no requiere una acción de detención.Puede especificar acciones de parada opcionales que se deben llevar a cabo en un evento o después de un periodo de tiempo.
Aplicar nueva configuración en <dispositivos>	Cambia los ajustes del dispositivo en uno o más dispositivos. Al seleccionar este tipo de acción, el asistente **Gestionar regla** le pide que seleccione dispositivos relevantes y puede definir los ajustes relevantes en los dispositivos que ha especificado.

Acción	Descripción
	 Si define ajustes para más de un dispositivo, solo puede cambiar los ajustes que están disponibles para todos los dispositivos especificados. **Ejemplo**: Especifique que la acción debe vincularse al Dispositivo 1 y al Dispositivo 2. El Dispositivo 1 tiene los ajustes A, B y C, y el Dispositivo 2 tiene los ajustes B, C y D. En este caso, solo puede cambiar los ajustes que están disponibles para ambos dispositivos, es decir, los ajustes B y C. **Ninguna acción de detención obligatoria**: Este tipo de acción no requiere una acción de detención.Puede especificar acciones de parada opcionales que se deben llevar a cabo en un evento o después de un periodo de tiempo.
Ajustar Matrix a vista <dispositivos>	Hace que el vídeo de las cámaras seleccionadas aparezca en un ordenador capaz de mostrar vídeo desencadenado por Matrix, como un ordenador en el que ha instalado XProtect Smart Client. Al seleccionar este tipo de acción, el asistente **Gestionar regla** le pide que seleccione un destinatario de Matrix, y uno o más dispositivos desde los que mostrar vídeo en el destinatario de Matrix seleccionado. Este tipo de acción le permite seleccionar solo un único destinatario de Matrix cada vez. Si quiere hacer que un vídeo de los dispositivos seleccionados aparezca en más de un destinatario de Matrix, debe crear una regla para cada destinatario Matrix requerido o utilice la característica XProtect Smart Wall. Al hacer clic con el botón derecho en una regla de la lista **Reglas**, puede copiar y reutilizar el contenido de las reglas. De este modo, puede evitar tener que crear reglas casi idénticas desde cero.

Acción	Descripción
	Como parte de la configuración en los ppropios destinatarios de Matrix, los usuarios deben especificar el número de puerto y la contraseña requeridos para la comunicación de Matrix. Asegúrese de que los usuarios tienen acceso a esta información. Normalmente los usuarios también deben definir las direcciones IP de los host permitidos desde los que se aceptan comandos relativos a la visualización de vídeo desencadenado por Matrix. En ese caso, los usuarios también deben conocer la dirección IP del servidor de gestión, o cualquier enrutador o cortafuegos utilizado.
Enviar captura SNMP	Genera un pequeño mensaje que registra eventos en dispositivos seleccionados. El texto las trampas de SNMP se genera automáticamente y no se puede personalizar. Puede contener el tipo de fuente y el nombre del dispositivo en el que se produjo el evento. **Ninguna acción de detención obligatoria**: Este tipo de acción no requiere una acción de detención.Puede especificar acciones de parada opcionales que se deben llevar a cabo en un evento o después de un periodo de tiempo.
Recuperar y almacenar grabaciones a distancia desde <dispositivos>.	Recupera y almacena grabaciones remotas de dispositivos seleccionados (que admiten grabaciones periféricas) en un periodo especificado antes y después del evento desencadenante. Esta regla es independiente del ajuste **Recuperar automáticamente grabaciones remotas cuando se restablece la conexión**. **Ninguna acción de detención obligatoria**: Este tipo de acción no requiere una acción de detención.Puede especificar acciones de parada opcionales que se deben llevar a cabo en un evento o después de un periodo de tiempo.
Recuperar y almacenar	Recupera y almacena grabaciones remotas en un periodo especificado desde dispositivos seleccionados (que admiten

Acción	Descripción
grabaciones a distancia entre <hora de inicio y fin> desde <dispositivos>.	grabaciones periféricas). Esta regla es independiente del ajuste **Recuperar automáticamente grabaciones remotas cuando se restablece la conexión**. **Ninguna acción de detención obligatoria**: Este tipo de acción no requiere una acción de detención.Puede especificar acciones de parada opcionales que se deben llevar a cabo en un evento o después de un periodo de tiempo.
Guardar imagen adjunta	Garantiza que, cuando se recibe una imagen del evento Imágenes recibidas (enviada por correo electrónico SMTP desde una cámara), se guarda para su uso futuro. En el futuro, otros eventos también pueden posiblemente desencadenar esta acción. **Ninguna acción de detención obligatoria**: Este tipo de acción no requiere una acción de detención.Puede especificar acciones de parada opcionales que se deben llevar a cabo en un evento o después de un periodo de tiempo.
Activar archivo en <archivos>	Inicia el archivado en uno o más archivos. Al seleccionar este tipo de acción, el asistente **Gestionar regla** le pide que seleccione archivos relevantes. **Ninguna acción de detención obligatoria**: Este tipo de acción no requiere una acción de detención.Puede especificar acciones de parada opcionales que se deben llevar a cabo en un evento o después de un periodo de tiempo.
En el <sitio>, active el <evento definido por el usuario>	Relevante principalmente en Milestone Federated Architecture, pero también puede usar esto en una configuración de un solo sitio. Utilice la regla para desencadenar un evento definido por usuarios en un sitio, normalmente un sitio remoto de una jerarquía federada. **Ninguna acción de detención obligatoria**: Este tipo de acción no requiere una acción de detención.Puede especificar acciones de parada opcionales que se deben llevar a cabo en un evento o después de un periodo de tiempo.
Mostrar <access request	Permite que las notificaciones de petición de acceso aparezcan en la pantalla de XProtect Smart Client cuando se cumplen los criterios de

Acción	Descripción
notification>	los eventos desencadenantes. Milestone le recomienda utilizar eventos de control de acceso como eventos desencadenantes para esta acción, porque las notificaciones de solicitud de acceso normalmente se configuran para funcionar en cámaras y comandos de control de acceso relacionados. Este tipo de acción requiere que tenga al menos un plug-in de control de acceso instalado en su sistema. **Ninguna acción de detención obligatoria**: Este tipo de acción no requiere una acción de detención.Puede especificar acciones de parada opcionales que se deben llevar a cabo en un evento o después de un periodo de tiempo.
Cambiar la contraseña en dispositivos de hardware	Cambia la contraseña de dispositivos de hardware seleccionados a una contraseña generada de forma aleatoria basada en los requisitos de la contraseña para ese dispositivo de hardware específico. Para ver una lista de dispositivos de hardware compatibles, consulte Buscar hardware. Esta acción solo está disponible al configurar una regla utilizando el tipo de regla **Realizar una acción en un <tiempo recurrente>**. Los siguientes eventos están disponibles para la acción: • Cambio de contraseña programado iniciado en la página 515 • Cambio de contraseña programado completado con éxito en la página 515 • Cambio de contraseña programado completado con errores en la página 515 Este tipo de acción no tiene una acción de parada. Puede ver el progreso de esta acción en el nodo **Tareas actuales**. Para obtener información adicional, consulte Ver tareas en curso actualmente en servidores de grabación en la página 300. Para ver los resultados de la acción, vaya al nodo **Registros del servidor** en la pestaña **Registros del sistema**. Si desea más

Acción	Descripción
	información, consulte Pestaña Registros del servidor (opciones) en la página 400. Para obtener informaciòn adicional, consulte Registros del sistema (pestaña).

Probar evento de análisis (propiedades)

Al probar los requisitos de un evento de análisis, aparece una ventana que comprueba cuatro condiciones y proporciona posibles descripciones de error y soluciones.

Condición	Descripción	Mensajes de error y soluciones
Cambios guardados	Si el evento es nuevo, ¿se ha guardado? O, si hay cambios en el nombre del evento, ¿se guardan esos cambios?	**Guarde los cambios antes de probar un evento de análisis**. Solución/Explicación: Guarde los cambios.
Eventos de análisis habilitados	¿Está habilitada la característica de Evento de análisis?	**Los eventos de análisis no se han habilitado**. Solución/Explicación: Habilite la característica de Eventos de análisis. Para hacerlo, haga clic en **Herramientas** > **Opciones** > **Eventos de análisis** y selecione la casilla de verificación **Habilitado**.
Dirección permitida	¿Está la dirección IP/el nombre del host de la máquina enviando el/los evento(s) permitidos (enumerados en la lista de direcciones de eventos de análisis)?	**El nombre de host local debe añadirse según lo permita la dirección para el servicio Evento de análisis**. Solución/Explicación: Añadir su máquina a la lista de direcciones de eventos de análisis de direcciones IP o nombres de host permitidos. **Error al resolver el nombre de host local**. Solución/Explicación: La dirección IP o el nombre de host de la máquina no se pueden encontrar o no son válidos.
Enviar evento de Analytics	¿Tuvo éxito el envío de un evento de prueba al Servidor de eventos?	Consulte la tabla siguiente.

Cada paso está marcado por un fallo en: ❌ o exitoso: ✓.

Mensajes de error y soluciones para la condición **Enviar evento de análisis**:

Mensaje de error	Solución
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 con el servidor de eventos en el puerto indicado. Lo más probable es que el error ocurra debido a problemas de red o a que el servicio Event Server se ha parado.
Error al enviar evento de análisis	Se establece la conexión con el servidor de eventos, pero el evento no se puede enviar. Lo más probable es que el error ocurra debido a problemas de red, por ejemplo, un tiempo de espera agotado.
Error al recibir respuestas del servidor de eventos	El evento se ha enviado al servidor de eventos, pero no se ha recibido respuesta. Lo más probable es que el error ocurra debido a problemas de red o a un puerto que está ocupado. Consulte el registro del servidor de eventos, normalmente ubicado en `ProgramData\Milestone\XProtect Event server\Logs\.`
Evento de análisis desconocido por el servidor de eventos	El servicio Event Server no conoce el evento. Lo más probable es que el error ocurra debido a que el evento o cambios en el evento no se han guardado.
Evento de análisis no válido recibido por el servidor de eventos	El formato del evento no es correcto.
Remitente no autorizado por servidor de eventos	Lo más probable es que su máquina no esté en la lista de direcciones IP o nombres de host permitidos.
Error interno en el servidor de eventos	Error del servidor de eventos. Consulte el registro del servidor de eventos, normalmente ubicado en `ProgramData\Milestone\XProtect Event server\Logs\.`

Mensaje de error	Solución
Respuesta no válida recibida del Servidor de eventos	La respuesta no es válida. Posiblemente el puerto está ocupado o hay problemas de red. Consulte el registro del servidor de eventos, normalmente ubicado en `ProgramData\Milestone\XProtect Event server\Logs\`.
Respuesta desconocida del servidor de eventos	La respuesta es válida, pero no se entiende. Posiblemente el error ocurre debido a problemas de red o a que el puerto está ocupado. Consulte el registro del servidor de eventos, normalmente ubicado en `ProgramData\Milestone\XProtect Event server\Logs\`.
Error inesperado	Póngase en contacto con el soporte de Milestone para recibir ayuda.

Eventos genéricos y fuentes de datos (propiedades)

Esta característica solo funciona si tiene el servidor de eventos de XProtect instalado.

Evento genérico (propiedades)

Componente	Requisito
Nombre	Nombre único para el evento genérico. El nombre debe ser único entre todos los tipos de eventos, como eventos definidos por el usuario, eventos de análisis, etc.
Habilitado	De forma predeterminada, los eventos genéricos están habilitados. Desactive la casilla de verificación para deshabilitar el evento.
Expresión	Expresión a la que debe estar atento el sistema al analizar paquetes de datos. Puede utilizar los siguientes operadores: • **( )**: Se utiliza para garantizar que los términos relacionados se procesan juntos como una unidad lógica. Se pueden utilizar para forzar determinado orden de procesamiento en el análisis **Ejemplo**: El criterio de búsqueda "(**Usuario001** O **Puerta053**) Y **Domingo**" primero procesa los dos términos entre paréntesis, luego combina el resultado con la última

Componente	Requisito
	parte de la cadena. Por tanto, el sistema primero busca cualquier paquete que contenga cualquiera de los términos **Usuario001** o **Puerta053**, luego toma los resultados y los revisa para ver qué paquetes también contienen el término **Domingo**. • **Y**: Con un operador AND, especifica que los términos a ambos lados del operador AND deben estar presentes **Ejemplo**: El criterio de búsqueda "**Usuario001** Y **Puerta053** Y **Domingo**" devuelve un resultado solo si los términos **Usuario001**, **Puerta053** y **Domingo** están todos incluidos en su expresión. No es suficiente que solo uno o dos de los términos estén presentes. Cuantos más términos combine con AND, menos resultados recupera. • **OR**: Con un operador OR, especifica que uno u otro término debe estar presente **Ejemplo**: El criterio de búsqueda "**Usuario001** O **Puerta053** O **Domingo**" devuelve cualquier resultado que contenga **Usuario001**, **Puerta053** o **Domingo**. Cuantos más términos combina con OR, más resultados recupera.
Tipos de expresión	Indica cómo de particular debe ser el sistema al analizar los paquetes de datos recibidos. Las opciones son las siguientes: • **Buscar**: Para que el evento se produzca, el paquete de datos recibido debe contener el texto especificado en el campo **Expresión**, pero también puede incluir más contenido **Ejemplo**: Si ha especificado que el paquete recibido debe contener los términos **Usuario001** y **Puerta053**, el evento se desencadena si el paquete recibido contiene los términos **Usuario001** y **Puerta053** y **Domingo**, ya que el paquete recibido contiene sus dos términos requeridos • **Coincidencia**: Para que el evento se produzca, el paquete de datos recibido debe contener exactamente el texto especificado en el campo **Expresión**, y nada más • **Expresión regular**: Para que el evento se produzca, el texto especificado en el campo **Expresión** debe identificar patrones específicos en los paquetes de datos recibidos Si cambia de **Buscar** o **Coincidir** a **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 (máxima prioridad) y 999999

Componente	Requisito
	(menor prioridad). El mismo paquete de datos puede ser analizado para distintos eventos. La capacidad para asignar una prioridad a cada evento le permite gestionar qué evento debe desencadenarse si un paquete recibido coincide con los criterios de varios eventos. Cuando el sistema recibe un paquete de TCP y/o UDP, comienza el análisis del paquete con el análisis del evento con la máxima prioridad. De este modo, cuando un paquete coincide con los criterios para varios eventos, solo se desencadena el evento con la prioridad más alta. Si un paquete coincide con los criterios para varios eventos con una prioridad idéntica, por ejemplo, dos eventos con una prioridad de 999, se desencadenan todos los eventos con esta prioridad.
Comprobar si la expresión coincide con la cadena de eventos	Se debe probar una cadena de eventos fente a la expresión introducida en el campo **Expresión**.

Fuente de datos de eventos genéricos (propiedades)

Componente	Requisito
Fuente de datos	Puede elegir entre dos fuentes de datos predeterminadas y definir una fuente de datos personalizada. Lo que elija depende de su programa de terceros y/o del hardware o software desde el que quiera interactuar: **Compatible**: Los ajustes predeterminados de fábrica están habilitados, refleja todos los bytes, TCP y UDP, solo IPv4, puerto 1234, sin separador, solo host local, codificación de página de códigos actual (ANSI). **Internacional**: Los ajustes predeterminados de fábrica están habilitados, refleja solo estadísticas, solo TCP, IPv4+6, puerto 1235, <CR><LF> como separador, solo host local, codificación UTF-8. (<CR><LF> = 13,10). [Fuente de datos A] [Fuente de datos B]

Componente	Requisito
	etc.
Nuevo	Haga clic para crear una nueva fuente de datos.
Nombre	Nombre de la fuente de datos.
Habilitado	Las fuentes de datos están habilitadas de forma predeterminada. Desactive la casilla de verificación para deshabilitar la fuente de datos.
Reiniciar	Haga clic para restablecer todos los ajustes para la fuente de datos seleccionada. El nombre introducido en el campo **Nombre** se mantiene.
Puerto	El número de puerto de la fuente de datos.
Selector del tipo de protocolo	Los protocolos a los que debe escuchar el sistema, y analizar, con el fin de detectar eventos genéricos: **Cualquiera**: TCP así como UDP. **TCP**: Solo TCP. **UDP**: Solo UDP. Los paquetes TCP y UDP utilizados para eventos genéricos pueden contener caracteres especiales, como @, #, +, ~ y más.
Selector de tipo de IP	Tipos de dirección IP seleccionables: IPv4, IPv6 o ambos.
Bytes de separador	Seleccione los bytes separadores utilizados para separar registros de eventos genéricos individuales. El valor predeterminado para el tipo de fuente de datos **Internacional** (consulte Fuente de datos en la página 534) es **13,10**. (13,10 = <CR><IF>).
Reflejar tipo de selector	Formatos de retorno de eco disponible:

Componente	Requisito
	• **Reflejar estadísticas**: Refleja el siguiente formato: **[X],[Y],[Z],[Nombre de evento genérico]** **[X]** = número de solicitud. **[Y]** = número de caracteres. **[Z]** = número de coincidencias con un evento genérico. **[Nombre del evento genérico]** = nombre introducido en el campo **Nombre** • **Reflejar todos los bytes**: Refleja todos los bytes • **Sin eco**: Suprime todo el eco
Selector del tipo de codificación	De forma predeterminada. la lista solo muestra las opciones más relevantes. Seleccione la casilla de verificación **Mostrar todo** para mostrar todas las opciones de condificación disponibles.
Mostrar todo	Consulte la viñeta anterior.
Direcciones IPv4 externas permitidas	Especifique las direcciones IP con las que el servidor de gestión debe comunicarse para gestionar eventos externos. También puede usar esto para excluir direcciones IP de las que no quiere datos.
Direcciones IPv6 externas permitidas	Especifique las direcciones IP con las que el servidor de gestión debe comunicarse para gestionar eventos externos. También puede usar esto para excluir direcciones IP de las que no quiere datos.

Los rangos pueden estar especificados en cada una de las cuatro posiciones, como **100,105,110-120**. Como ejemplo, todas las direcciones de la red 10,10 se pueden permitir mediante **10.10.[0-254].[0-254]** o **10.10.255.255**.

Webhooks (nodo Reglas y Eventos)

En el nodo **Webhooks**, puede crear, editar y eliminar puntos finales webhook.

Los siguientes campos están disponibles al crear y editar webhooks:

Campo	Descripción
Nombre	Introduzca un nombre único del punto final webhook. El nombre de webhook no puede estar vacío.
Dirección	El URL del servidor web o aplicación al que desea enviar datos de eventos. Si se actualiza el URL del servidor web, debe actualizar el webhook URL en el nodo webhook. El uso de HTTP a través de redes no seguras (como Internet abierto) expone todos los eventos en texto sin formato.
Token	Introduzca un token que se utilice para ayudar a asegurar la comunicación con otras aplicaciones validando la fuente de la PUBLICACIÓN HTTP. El uso de un token para proteger la comunicación es opcional, pero se recomienda.
Versión de API	La versión del plug-in webhook y la API utilizada para la funcionalidad webhook.

Nodo Seguridad

Roles (nodo Seguridad)

Pestaña Información (roles)

La funcionalidad disponible depende del sistema que esté utilizando. Vea la lista completa de características, que está disponible en la página de descripción del producto en el sitio web Milestone (https://www.milestonesys.com/solutions/platform/product-index/).

En la pestaña **Información** de un rol, puede establecer lo siguiente:

Nombre	Descripción
Nombre	Introduzca un nombre para el rol.
Descripción	Introduzca una descripción para el rol.
Perfil de Management Client	Seleccione un perfil de Management Client para asociarlo al rol. No puede aplicar esto al rol de **Administradores** predeterminado.  Requiere permisos para gestionar la seguridad en el servidor de gestión.
Perfil de Smart Client	Seleccione un perfil de Smart Client para asociarlo al rol.  Requiere permisos para gestionar la seguridad en el servidor de gestión.
Perfil temporal predeterminado	Seleccione un perfil temporal predeterminado para asociarlo al rol. No puede aplicar esto al rol de **Administradores** predeterminado.
Perfil de bloqueo de evidencias	Seleccione un perfil de bloqueo de evidencias para asociarlo al rol.
Inicio de sesión en Smart Client en el perfil temporal	Seleccione un perfil temporal para el que el usuario de XProtect Smart Client asociado a este rol tiene permitido iniciar sesión. Si el usuario de XProtect Smart Client ha iniciado sesión cuando el periodo vence, su sesión se cierra de forma automática. No puede aplicar esto al rol de **Administradores** predeterminado.
Permitir inicio de sesión en Smart Client	Seleccione la casilla de verificación para permitir a los usuarios asociados a este rol iniciar sesión en XProtect Smart Client. El acceso a Smart Client no está permitido de forma predeterminada. Desactive la casilla de verificación para denegar el acceso a XProtect Smart Client.
Permitir inicio de	Seleccione la casilla de verificación para permitir a los usuarios asociados a este

Nombre	Descripción
sesión en el cliente de XProtect Mobile	rol iniciar sesión en el cliente XProtect Mobile. El acceso al cliente de XProtect Mobile no está permitido de forma predeterminada. Desactive la casilla de verificación para denegar el acceso al cliente de XProtect Mobile.
Permitir inicio de sesión en XProtect Web Client	Seleccione la casilla de verificación para permitir a los usuarios asociados a este rol iniciar sesión en XProtect Web Client. El acceso a XProtect Web Client no está permitido de forma predeterminada. 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 inicio de sesión con el rol. Quiere decir que XProtect Smart Client o el Management Client pidan una segunda autorización,normalmente por un superusuario o gerente, cuando el usuario inicie sesión. Para habilitar a los administradores para que autoricen a los usuarios, configure el permiso **Autorizar usuarios** del servidor de gestión en la pestaña **Seguridad general**. No puede aplicar esto al rol de **Administradores** predeterminado.
Hacer que los usuarios sean anónimos durante las sesiones PTZ	Seleccione la casilla de verificación para ocultar los nombres de los usuarios asociados a este rol cuando controlen sesiones PTZ.

Pestaña Usuario y Grupos (roles)

En la pestaña **Usuario y Grupos**, asigne usuarios y grupos a roles (consulte Asignar/eliminar usuarios y grupos a/de roles en la página 296). Puede asignar usuarios y grupos de Windows o usuarios básicos (consulte Usuarios (explicación) en la página 64).

IDP externo (cometidos)

En la pestaña **IDP externo**, puede ver las reclamaciones existentes y añadir nuevas reclamaciones a los cometidos.

Nombre	Descripción
IDP externo	El nombre del IDP externo.
Nombre de la reclamación	Una variable que está definida en el IDP externo.
Valor de la reclamación	El valor de la reclamación, como un nombre de grupo, que puede utilizarse para asignar los cometidos adecuados al usuario.

Pestaña Seguridad global (roles)

La funcionalidad disponible depende del sistema que esté utilizando. Vea la lista completa de características, que está disponible en la página de descripción del producto en el sitio web Milestone (https://www.milestonesys.com/solutions/platform/product-index/).

En la pestaña **Seguridad general**, se configuran los permisos generales para los cometidos. Para cada componente disponible en su sistema, defina los permisos de acceso para los cometidos estableciendo **Permitir** o **Denegar**. Cuando a un rol se le deniega el acceso a un componente, ese componente no es visible en la pestaña **Seguridad global** para un usuario en ese rol.

La pestaña **Seguridad general** no está disponible en el XProtect Essential+ gratuito.

Puede definir más permisos de acceso para XProtect Corporate que para los demás XProtect productos VMS. Esto se debe a que solo puede configurar permisos de administrador diferenciados en XProtect Corporate, mientras que puede configurar permisos generales para un cometido que utilice XProtect Smart Client, o XProtect Web Client cliente XProtect Mobile en todos los productos.

Los ajustes de seguridad global solo se aplican al sitio actual.

Si asocia un usuario con más de un cometido y selecciona **Denegar** en una configuración de seguridad para un cometido y **Permitir** para otro, el permiso **Denegar** anula el permiso **Permitir**.

A continuación, las descripciones muestran lo que ocurre en cada permiso individual para los diferentes componentes del sistema si se selecciona **Permitir** para los cometidos correspondientes. Si utiliza XProtect Corporate, puede ver qué ajustes hay disponibles **solo** para su sistema en cada componente del sistema.

Para cada componente o funcionalidad del sistema, el administrador del sistema entero puede usar las casillas de verificación **Permitir** o **Denegar** para configurar permisos de seguridad para el rol. Cualquier permiso de seguridad que configure aquí se configurará para todo componente o funcionalidad del sistema. Si, por ejemplo, selecciona la casilla de verificación **Denegar** en **Cámaras**, todas las cámaras añadidas al sistema no están disponibles para el rol. Em contraste, si selecciona la casilla de verificación **Permitir**, el rol puede ver todas las cámaras añadidas al sistema. El resultado de seleccionar **Permitir** o **Denegar** en sus cámaras es que los ajustes de la cámara en la pestaña **Dispositivo** heredan entonces las selecciones de la pestaña **Seguridad global** de modo que todas las cámaras estén disponibles o no disponibles para el rol concreto.

Si quiere establecer permisos de seguridad para cámaras **individuales** o similar, solo puede establecer estos permisos individuales en la pestaña del componente o la funcionalidad del sistema relevante si **no ha establecido ningún permiso general** para el componente o la funcionalidad del sistema en la pestaña **Seguridad global**.

Las descripciones que aparecen a continuación también se aplican a los permisos que puede configurar a través de los MIP SDK.

Si quiere cambiar su licencia básica de XProtect Corporate a uno de los otros productos, asegúrese de que elimina todos los permisos de seguridad que están disponibles solo para XProtect Corporate. Si no elimina esos permisos, no podrá completar el cambio.

Management Server

La funcionalidad disponible depende del sistema que esté utilizando. Vea la lista completa de características, que está disponible en la página de descripción del producto en el sitio web Milestone (https://www.milestonesys.com/solutions/platform/product-index/).

Permiso de seguridad	Descripción
Control total	Habilita el permiso para gestionar todas las entradas de seguridad en esta parte del sistema.
Conectar	Habilita a los usuarios a conectarse a Management Server. Este permiso está habilitado de forma predeterminada. Puede denegar temporalmente el permiso de conexión en roles con fines de mantenimiento y, a continuación, volver a solicitar el acceso al sistema.

Permiso de seguridad	Descripción
	⚠ Este permiso debe estar seleccionado para permitir el acceso al sistema.
Leer	⚠ Este permiso es un permiso administrativo altamente privilegiado que otorga importantes derechos de acceso a XProtect VMS, incluido el acceso a datos confidenciales, como las credenciales configuradas en el sistema. Habilita el permiso para acceder a una amplia gama de funcionalidades, incluyendo: • Iniciando sesión en el Management Client • Lista de tareas actuales • Registros de servidores También habilita el acceso a: • Servicios de conexión remota • Perfiles Smart Client • Perfiles Management Client • Matrix • Perfiles temporales • Servidores registrados y API de registro de servicios Este permiso también revela cierta información confidencial al cliente: • Credenciales para cualquier IDP externo configurado • Credenciales, direcciones IP y otra información para todas las cámaras en el XProtect VMS • Credenciales para el servidor de correo configurado • Credenciales para cualquier matrix configurada • Credenciales configuradas para la caracteristica de Interconnect • Credenciales configuradas para activación de licencia

Permiso de seguridad	Descripción
	Este permiso no revela las credenciales de los usuarios de XProtect VMS. Esto incluye usuarios básicos, usuarios Windows y usuarios de IDP externo.
Editar	Habilita el permiso para modificar los datos en una amplia gama de funcionalidades, incluyendo: • Opciones • Gestión de licencias También habilita a los usuarios a crear, eliminar y editar lo siguiente: • Servicios de conexión remota • Grupos de dispositivos • Matrix • Perfiles temporales • Perfiles de notificación • Servidores registrados  Habilita el permiso para configurar rangos de IP locales al configurar la red en el servidor de grabación.
Monitor del sistema	Habilita el permiso para ver los datos del Monitor del sistema.
API de estado	Habilita el permiso para realizar consultas en la API de estado ubicada en el servidor de grabación. Esto significa que los cometidos con este permiso habilitado tienen acceso a leer el estado de los elementos ubicados en el servidor de grabación.
Gestionar jerarquía de sitios federados	Habilita el permiso para añadir y desvincular el sitio actual a otros sitios en una jerarquía de sitios federados.  Si establece este permiso en permitido únicamente en el sitio secundario, el usuario aún puede desvincular el sitio del sitio principal.

Permiso de seguridad	Descripción
Configuración de la copia de seguridad	Habilita el permiso para crear copias de seguridad de la configuración del sistema utilizando la funcionalidad de copia de seguridad y restauración del sistema.
Autorizar usuarios	Habilita el permiso para autorizar a los usuarios cuando se les pide un segundo inicio de sesión en XProtect Smart Client o Management Client. Si un cometido requiere autorización de inicio de sesión se define en la pestaña **Información**.
Gestionar seguridad	Habilita el permiso para gestionar los permisos del Servidor de gestión. También habilita a los usuarios a crear, eliminar y editar las siguientes características: • Cometidos • Usuarios básicos • Perfiles Smart Client • Perfiles Management Client

Servidores de grabación

La funcionalidad disponible depende del sistema que esté utilizando. Vea la lista completa de características, que está disponible en la página de descripción del producto en el sitio web Milestone (https://www.milestonesys.com/solutions/platform/product-index/).

Permiso de seguridad	Descripción
Control total	Habilita el permiso para gestionar todas las entradas de seguridad en esta parte del sistema.
Editar	Habilita el permiso para editar las propiedades en los servidores de grabación, excepto los ajustes de configuración de red que requieren permiso de edición en

Permiso de seguridad	Descripción
	el servidor de gestión.
Borrar	Habilita el permiso para eliminar los servidores de grabación. Para ello, también debe dar al usuario permisos de eliminación en: • Grupo de seguridad de hardware si ha añadido hardware al servidor de grabación Si alguno de los dispositivos en el servidor de grabación contiene bloqueos de evidencias, solo puede eliminar el servidor de grabación si está fuera de línea.
Gestionar hardware	Habilita el permiso para añadir hardware en los servidores de grabación.
Gestionar almacenamiento	Habilita el permiso para administrar contenedores de almacenamiento en el servidor de grabación, es decir, para crear, eliminar, mover y vaciar contenedores de almacenamiento.
Gestionar seguridad	Habilita el permiso para gestionar los permisos de seguridad de los servidores de grabación.

Servidores failover

La funcionalidad disponible depende del sistema que esté utilizando. Vea la lista completa de características, que está disponible en la página de descripción del producto en el sitio web Milestone (https://www.milestonesys.com/solutions/platform/product-index/).

Permiso de seguridad	Descripción
Control total	Habilita el permiso para gestionar todas las entradas de seguridad en esta parte del sistema.

Permiso de seguridad	Descripción
Leer	Habilita el permiso para ver y acceder a los servidores de failover en el Management Client.
Editar	Habilita el permiso para crear, actualizar, eliminar, mover y habilitar o deshabilitar servidores de failover en el Management Client.
Gestionar seguridad	Habilita el permiso para gestionar los permisos de seguridad de los servidores de failover.

Servidores Mobile

La funcionalidad disponible depende del sistema que esté utilizando. Vea la lista completa de características, que está disponible en la página de descripción del producto en el sitio web Milestone (https://www.milestonesys.com/solutions/platform/product-index/).

Permiso de seguridad	Descripción
Control total	Habilita el permiso para gestionar todas las entradas de seguridad en esta parte del sistema.
Leer	Habilita el permiso para ver y acceder a los servidores móviles en el Management Client.
Editar	Habilita el permiso para editar y eliminar servidores móviles en el Management Client.
Gestionar seguridad	Habilita el permiso para gestionar los permisos de seguridad de los servidores móviles.
Crear	Habilita el permiso para añadir servidores móviles al sistema.

Hardware

La funcionalidad disponible depende del sistema que esté utilizando. Vea la lista completa de características, que está disponible en la página de descripción del producto en el sitio web Milestone (https://www.milestonesys.com/solutions/platform/product-index/).

Permiso de seguridad	Descripción
Control total	Habilita el permiso para gestionar todas las entradas de seguridad en esta parte del sistema.
Editar	Habilita el permiso para editar las propiedades del hardware.
Borrar	Habilita el permiso para eliminar el hardware. Si alguno de los dispositivos de hardware contiene bloqueos de evidencias, solo puede eliminar el hardware si el servidor de grabación está fuera de línea.
Comandos de driver	Habilita el permiso para enviar comandos especiales a los controladores y así controlar las características y la configuración en el propio dispositivo. El permiso de los **Comandos de driver** es solo para los plug-in MIP desarrollados especialmente en los clientes. No controla tareas de configuración estándar.
Ver contraseñas	Habilita el permiso para ver las contraseñas de los dispositivos de hardware en el cuadro de diálogo **Editar hardware**.
Gestionar seguridad	Habilita el permiso para gestionar los permisos de seguridad del hardware.

Cámaras

La funcionalidad disponible depende del sistema que esté utilizando. Vea la lista completa de características, que está disponible en la página de descripción del producto en el sitio web Milestone (https://www.milestonesys.com/solutions/platform/product-index/).

Permiso de seguridad	Descripción
Control total	Habilita el permiso para gestionar todas las entradas de seguridad en esta parte del sistema.
Leer	Habilita el permiso para ver los dispositivos de la cámara en los clientes y el Management Client.
Editar	Habilita el permiso para editar las propiedades de las cámaras en el Management Client. También habilita a los usuarios a habilitar o deshabilitar una cámara.
Ver en directo	Habilita el permiso para ver el vídeo en directo de las cámaras de los clientes y el Management Client.
Ver directo restringido	Habilita el permiso para ver el vídeo en directo restringido de las cámaras de los clientes y el Management Client.
Reproducción	Habilita el permiso para reproducir el vídeo grabado de las cámaras en todos los clientes.
Reproducción de grabaciones restringidas	Habilita el permiso para reproducir el vídeo grabado restringido de las cámaras en todos los clientes.
Recuperar grabaciones a distancia	Habilita el permiso para recuperar las grabaciones en los clientes de las cámaras en sitios remotos o de los almacenamientos de borde en las cámaras.
Leer secuencias	Habilita el permiso para leer la información de la secuencia relacionada, por ejemplo, con la reproducción de vídeos grabados en los clientes.
Búsqueda avanzada	Habilita el permiso para utilizar la función de búsqueda inteligente en los clientes.

Permiso de seguridad	Descripción
Exportar	Habilita el permiso para exportar las grabaciones de los clientes.
Crear marcador	Habilita el permiso para crear marcadores en los vídeos grabados y en directo en los clientes.
Leer marcadores	Habilita el permiso para buscar y leer los detalles de los marcadores en los clientes.
Editar marcadores	Habilita el permiso para editar los marcadores en los clientes.
Eliminar marcadores	Habilita el permiso para eliminar marcadores en los clientes.
Crear y ampliar bloqueos de evidencias	Habilita el permiso para crear y ampliar los bloqueos de evidencia en los clientes.
Leer bloqueo de evidencias	Habilita el permiso para buscar y leer bloqueos de evidencia en los clientes.
Eliminar y reducir bloqueos de evidencias	Habilita el permiso para eliminar o reducir los bloqueos de evidencias en los clientes.
Crear y ampliar restricciones en vivo y para la reproducción	Habilita el permiso para crear y ampliar restricciones en los clientes.
Leer restricciones en directo y para la reproducción	Habilita el permiso para ver una lista de restricciones existentes en los clientes.
Eliminar y reducir restricciones en directo y para la reproducción	Habilita el permiso para eliminar o reducir restricciones en los clientes.
Iniciar la grabación manual	Habilita el permiso para iniciar la grabación manual de vídeo en los clientes.
Detener la grabación manual	Habilita el permiso para detener la grabación manual de vídeo en los clientes.

Permiso de seguridad	Descripción
Comandos AUX	Habilita el permiso para utilizar comandos auxiliares (AUX) en la cámara desde los clientes. Los **comandos AUX** ofrecen a los usuarios control de, por ejemplo, los limpiaparabrisas de una cámara conectados mediante un codificador de vídeo. Los dispositivos asociados a la cámara conectados mediante conexiones auxiliares se controlan desde el cliente.
PTZ manual	Habilita el permiso para utilizar las funciones PTZ en las cámaras PTZ de los clientes y el Management Client.
Activar valores preestablecidos PTZ o perfiles de patrulla	Habilita el permiso para mover las cámaras PTZ a posiciones preestablecidas, iniciar y detener los perfiles de patrulla, y pausar una patrulla en los clientes y el Management Client. Para permitir que este cometido utilice otras funciones PTZ en la cámara, habilite el permiso **PTZ manual**.
Gestionar valores preestablecidos PTZ o perfiles de patrulla	Habilita el permiso para añadir, editar y eliminar valores preestablecidos de PTZ y perfiles de patrulla en las cámaras PTZ de los clientes y el Management Client. Para permitir que este cometido utilice otras funciones PTZ en la cámara, habilite el permiso **PTZ manual**.
Bloquear/Desbloquear valores preestablecidos PTZ	Habilita el permiso para bloquear y desbloquear valores preestablecidos de PTZ en el Management Client. Esto evita o permite que otros usuarios cambien posiciones preestablecidas en los clientes y en el Management Client.
Reservar sesiones PTZ	Habilita el permiso para poner las cámaras PTZ en modo de sesión PTZ reservada en los clientes y el Management Client. En una sesión PTZ reservada, otros usuarios con una mayor prioridad de PTZ no pueden asumir el control. Para permitir que este cometido utilice otras funciones PTZ en la cámara, habilite el permiso **PTZ manual**.
Liberar sesione PTZ	Habilita el permiso para liberar las sesiones PTZ de otros usuarios

Permiso de seguridad	Descripción
	del Management Client. Siempre puede liberar sus propias sesiones de PTZ - sin este permiso.
Borrar grabaciones	Habilita el permiso para eliminar del sistema las grabaciones de vídeo almacenadas a través del Management Client.
Retirar máscaras de privacidad	Habilita el permiso para levantar temporalmente las máscaras de privacidad en XProtect Smart Client. También habilita el permiso para autorizar a otros usuarios de XProtect Smart Client a levantar las máscaras de privacidad. El levantamiento de máscaras de privacidad solo se aplica a máscaras de privacidad configuradas como máscaras de privacidad levantables en el Management Client.
Gestionar seguridad	Habilita el permiso para gestionar los permisos de seguridad en el Management Client para la cámara.

Micrófonos

La funcionalidad disponible depende del sistema que esté utilizando. Vea la lista completa de características, que está disponible en la página de descripción del producto en el sitio web Milestone (https://www.milestonesys.com/solutions/platform/product-index/).

Permiso de seguridad	Descripción
Control total	Habilita el permiso para gestionar todas las entradas de seguridad en esta parte del sistema.

Permiso de seguridad	Descripción
Leer	Habilita el permiso para ver los dispositivos de micrófono en los clientes y el Management Client.
Editar	Habilita el permiso para editar las propiedades del micrófono en el Management Client. También permite a los usuarios habilitar o deshabilitar micrófonos.
Escucha en directo	Habilita el permiso para escuchar el audio en directo de los altavoces de los clientes y el Management Client.
Escuchar audio en directo restringido	Habilita el permiso para escuchar el audio en directo de los altavoces de los clientes y el Management Client.
Reproducción	Habilita el permiso para reproducir el audio grabado de los micrófonos de los clientes.
Reproducción de grabaciones restringidas	Habilita el permiso para reproducir el audio grabado restringido de los micrófonos de los clientes.
Recuperar grabaciones a distancia	Habilita el permiso para recuperar las grabaciones en los clientes desde los micrófonos de los sitios remotos o desde los almacenes de borde de las cámaras.
Leer secuencias	Habilita el permiso para leer la información de la secuencia relacionada, por ejemplo, con la pestaña **Reproducción** en los clientes.
Exportar	Habilita el permiso para exportar las grabaciones de los clientes.
Crear marcador	Habilita el permiso para crear marcadores en los clientes.
Leer marcadores	Habilita el permiso para buscar y leer los detalles de los marcadores en los clientes.
Editar marcadores	Habilita el permiso para editar los marcadores en los clientes.

Permiso de seguridad	Descripción
Eliminar marcadores	Habilita el permiso para eliminar marcadores en los clientes.
Crear y ampliar bloqueos de evidencias	Habilita el permiso para crear o ampliar los bloqueos de evidencia en los clientes.
Leer bloqueo de evidencias	Habilita el permiso para buscar y leer los detalles del bloqueo de evidencia en los clientes.
Eliminar y reducir bloqueos de evidencias	Habilita el permiso para eliminar o reducir los bloqueos de evidencias en los clientes.
Crear y ampliar restricciones en vivo y para la reproducción	Habilita el permiso para crear y ampliar restricciones en los micrófonos de los clientes.
Leer restricciones en directo y para la reproducción	Habilita el permiso para ver una lista de las restricciones existentes en los micrófonos de los clientes.
Eliminar y reducir restricciones en directo y para la reproducción	Habilita el permiso para eliminar y reducir las restricciones de los micrófonos en los clientes.
Iniciar la grabación manual	Habilita el permiso para iniciar la grabación manual de audio en los clientes.
Detener la grabación manual	Habilita el permiso para detener la grabación manual de audio en los clientes.
Borrar	Habilita el permiso para eliminar del sistema las grabaciones

Permiso de seguridad	Descripción
grabaciones	almacenadas.
Gestionar seguridad	Habilita el permiso para gestionar los permisos de seguridad en el Management Client para los micrófonos.

Altavoces

La funcionalidad disponible depende del sistema que esté utilizando. Vea la lista completa de características, que está disponible en la página de descripción del producto en el sitio web Milestone (https://www.milestonesys.com/solutions/platform/product-index/).

Permiso de seguridad	Descripción
Control total	Habilita el permiso para gestionar todas las entradas de seguridad en esta parte del sistema.
Leer	Habilita el permiso para ver los dispositivos de altavoz en los clientes y el Management Client.
Editar	Habilita el permiso para editar las propiedades de los altavoces en el Management Client. También permite a los usuarios habilitar o deshabilitar altavoces.
Oír en directo	Habilita el permiso para escuchar el audio en directo de los altavoces de los clientes y el Management Client.
Escuchar audio en directo restringido	Habilita el permiso para escuchar el audio en directo de los altavoces de los clientes y el Management Client.
Hablar	Habilita el permiso para hablar a través de los altavoces de los clientes.

Permiso de seguridad	Descripción
Reproducción	Habilita el permiso para reproducir el audio grabado desde los altavoces de los clientes.
Reproducción de grabaciones restringidas	Habilita el permiso para reproducir el audio grabado desde los altavoces de los clientes.
Recuperar grabaciones a distancia	Habilita el permiso para recuperar las grabaciones en los clientes de los altavoces en los sitios remotos o de los almacenamientos de borde en las cámaras.
Leer secuencias	Habilita el permiso para utilizar la función de Secuencias mientras explora el audio grabado de los altavoces en los clientes.
Exportar	Habilita el permiso para exportar el audio grabado de los altavoces en los clientes.
Crear marcador	Habilita el permiso para crear marcadores en los clientes.
Leer marcadores	Habilita el permiso para buscar y leer los detalles de los marcadores en los clientes.
Editar marcadores	Habilita el permiso para editar los marcadores en los clientes.
Eliminar marcadores	Habilita el permiso para eliminar marcadores en los clientes.
Crear y ampliar bloqueos de evidencias	Habilita el permiso para crear o ampliar los bloqueos de evidencia para proteger el audio grabado en los clientes.
Leer bloqueo de evidencias	Habilita el permiso para ver el audio grabado protegido por bloqueos de evidencia en los clientes.
Eliminar y reducir bloqueos de	Habilita el permiso para eliminar o reducir los bloqueos de evidencia en el audio protegido de los clientes.

Permiso de seguridad	Descripción
evidencias	
Crear y ampliar restricciones en vivo y para la reproducción	Habilita el permiso para crear y ampliar restricciones en los altavoces de los clientes.
Leer restricciones en directo y para la reproducción	Habilita el permiso para ver una lista de las restricciones existentes en los altavoces de los clientes.
Eliminar y reducir restricciones en directo y para la reproducción	Habilita el permiso para eliminar y reducir las restricciones de los altavoces en los clientes.
Iniciar la grabación manual	Habilita el permiso para iniciar la grabación manual de audio en los clientes.
Detener la grabación manual	Habilita el permiso para detener la grabación manual de audio en los clientes.
Borrar grabaciones	Habilita el permiso para eliminar del sistema las grabaciones almacenadas.
Gestionar seguridad	Habilita el permiso para gestionar los permisos de seguridad en el Management Client para los altavoces.

Metadatos

La funcionalidad disponible depende del sistema que esté utilizando. Vea la lista completa de características, que está disponible en la página de descripción del producto en el sitio web Milestone (https://www.milestonesys.com/solutions/platform/product-index/).

Permiso de seguridad	Descripción
Control total	Habilita el permiso para gestionar todas las entradas de seguridad en esta parte del sistema.
Leer	Habilita el permiso para recibir metadatos en los clientes.
Editar	Habilita el permiso para editar las propiedades de los metadatos en el Management Client. También permite a los usuarios habilitar o deshabilitar dispositivos de metadatos.
Directo	Habilita el permiso para recibir metadatos en directo de los dispositivos de metadatos de los clientes.
Ver directo restringido	Habilita el permiso para recibir metadatos restringidos en directo de los dispositivos de metadatos de los clientes.
Reproducción	Habilita el permiso para reproducir los datos grabados de los dispositivos de metadatos en los clientes.
Reproducción de grabaciones restringidas	Habilita el permiso para reproducir los datos grabados restringidos de los dispositivos de metadatos en los clientes.
Recuperar grabaciones a distancia	Habilita el permiso para recuperar las grabaciones en los clientes de los dispositivos de metadatos en sitios remotos o de los almacenamientos de borde en las cámaras.
Leer secuencias	Habilita el permiso para leer la información de la secuencia relacionada, por ejemplo, con la pestaña **Reproducción** en los clientes.
Exportar	Habilita el permiso para exportar grabaciones en los clientes.
Crear y ampliar bloqueos de evidencias	Habilita el permiso para crear bloqueos de evidencia en los clientes.
Leer bloqueo de evidencias	Habilita el permiso para ver los bloqueos de evidencia en los clientes.

Permiso de seguridad	Descripción
Eliminar y reducir bloqueos de evidencias	Habilita el permiso para eliminar o reducir los bloqueos de evidencias en los clientes.
Crear y ampliar restricciones en vivo y para la reproducción	Habilita el permiso para crear y ampliar las restricciones en los metadatos de los clientes.
Leer restricciones en directo y para la reproducción	Habilita el permiso para ver una lista de las restricciones existentes en los metadatos de los clientes.
Eliminar y reducir restricciones en directo y para la reproducción	Habilita el permiso para eliminar o reducir las restricciones en los metadatos de los clientes.
Iniciar la grabación manual	Habilita el permiso para iniciar la grabación manual de metadatos en los clientes.
Detener la grabación manual	Habilita el permiso para detener la grabación manual de metadatos en los clientes.
Borrar grabaciones	Habilita el permiso para eliminar del sistema las grabaciones almacenadas.
Gestionar seguridad	Habilita el permiso para gestionar los permisos de seguridad en el Management Client para metadatos.

Entrada

La funcionalidad disponible depende del sistema que esté utilizando. Vea la lista completa de características, que está disponible en la página de descripción del producto en el sitio web Milestone (https://www.milestonesys.com/solutions/platform/product-index/).

Permiso de seguridad	Descripción
Control total	Habilita el permiso para gestionar todas las entradas de seguridad en esta parte del sistema.
Leer	Habilita el permiso para ver los dispositivos de entrada en los clientes y el Management Client.
Editar	Habilita el permiso para editar las propiedades de los dispositivos de entrada en el Management Client. También habilita a los usuarios a habilitar o deshabilitar un dispositivo de entrada.
Gestionar seguridad	Habilita el permiso para gestionar los permisos de seguridad en el Management Client para dispositivos de entrada.

Salida

La funcionalidad disponible depende del sistema que esté utilizando. Vea la lista completa de características, que está disponible en la página de descripción del producto en el sitio web Milestone (https://www.milestonesys.com/solutions/platform/product-index/).

Permiso de seguridad	Descripción
Control total	Habilita el permiso para gestionar todas las entradas de seguridad en esta parte del sistema.

Permiso de seguridad	Descripción
Leer	Habilita el permiso para ver los dispositivos de salida en los clientes.
Editar	Habilita el permiso para editar las propiedades de los dispositivos de salida en el Management Client. También habilita a los usuarios a habilitar o deshabilitar un dispositivo de salida.
Activar	Habilita el permiso para activar las salidas en los clientes.
Gestionar seguridad	Habilita el permiso para gestionar los permisos de seguridad en el Management Client para los dispositivos de salida.

Smart Wall

La funcionalidad disponible depende del sistema que esté utilizando. Vea la lista completa de características, que está disponible en la página de descripción del producto en el sitio web Milestone (https://www.milestonesys.com/solutions/platform/product-index/).

Permiso de seguridad	Descripción
Control total	Habilita el permiso para gestionar todos los permisos de seguridad en XProtect Management Client.
Leer	Habilita el permiso para ver un panel de vídeo en XProtect Smart Client.
Editar	Habilita el permiso para editar las propiedades de la definición Smart Wall en XProtect Management Client.
Borrar	Habilita el permiso para eliminar las definiciones existentes Smart Wall en XProtect Management Client.
Operar	Habilita el permiso para activar y modificar definiciones Smart Wall, por ejemplo

Permiso de seguridad	Descripción
	para cambiar y activar valores preestablecidos o aplicar cámaras en XProtect Smart Client y en XProtect Management Client. Puede asociar **Operar** con perfiles temporales que definen cuándo se aplica el permiso del usuario.
Crear Smart Wall	Habilita el permiso para crear nuevas definiciones de Smart Wall en XProtect Management Client.
Gestionar seguridad	Habilita el permiso para gestionar los permisos de seguridad en XProtect Management Client para la definición de Smart Wall.
Reproducción	Habilita el permiso para reproducir los datos grabados de un panel de vídeo en XProtect Smart Client. Puede asociar **Reproducción** con perfiles temporales que definen cuándo se aplica el permiso del usuario.

Grupos de vistas

La funcionalidad disponible depende del sistema que esté utilizando. Vea la lista completa de características, que está disponible en la página de descripción del producto en el sitio web Milestone (https://www.milestonesys.com/solutions/platform/product-index/).

Permiso de seguridad	Descripción
Control total	Habilita el permiso para gestionar todas las entradas de seguridad en esta parte del sistema.

Permiso de seguridad	Descripción
Leer	Habilita el permiso para ver los Grupos de vista en los clientes y en el Management Client. Los grupos de vistas se crean en el Management Client.
Editar	Habilita el permiso para editar las propiedades de los Grupos de vista en el Management Client.
Borrar	Habilita el permiso para eliminar Grupos de vista en el Management Client.
Operar	Habilita el permiso para utilizar los grupos de vistas en XProtect Smart Client, es decir, para crear y eliminar subgrupos y vistas.
Crear grupo de vistas	Habilita el permiso para crear Grupos de vista en el Management Client.
Gestionar seguridad	Habilita el permiso para gestionar los permisos de seguridad en el Management Client para los Grupos de vista.

Eventos definidos por el usuario

La funcionalidad disponible depende del sistema que esté utilizando. Vea la lista completa de características, que está disponible en la página de descripción del producto en el sitio web Milestone (https://www.milestonesys.com/solutions/platform/product-index/).

Permiso de seguridad	Descripción
Control total	Habilita el permiso para gestionar todas las entradas de seguridad en esta parte del sistema.
Leer	Habilita el permiso para ver los eventos definidos por el usuario en los clientes.
Editar	Habilita el permiso para editar las propiedades de los eventos definidos por el

Permiso de seguridad	Descripción
	usuario en el Management Client.
Borrar	Habilita el permiso para eliminar eventos definidos por el usuario en el Management Client.
Activador	Habilita el permiso para activar eventos definidos por el usuario en los clientes.
Gestionar seguridad	Habilita el permiso para gestionar los permisos de seguridad en el Management Client para eventos definidos por el usuario.
Crear evento definido por el usuario	Habilita el permiso para crear nuevos eventos definidos por el usuario en el Management Client.

Eventos de Analytics

La funcionalidad disponible depende del sistema que esté utilizando. Vea la lista completa de características, que está disponible en la página de descripción del producto en el sitio web Milestone (https://www.milestonesys.com/solutions/platform/product-index/).

Permiso de seguridad	Descripción
Control total	Habilita el permiso para gestionar todas las entradas de seguridad en esta parte del sistema.
Leer	Habilita el permiso para ver los eventos de análisis en el Management Client.
Editar	Habilita el permiso para editar las propiedades de los eventos de análisis en el Management Client.
Gestionar seguridad	Habilita el permiso para gestionar los permisos de seguridad en el Management Client para los eventos de análisis.

Eventos genéricos

Permiso de seguridad	Descripción
Control total	Habilita el permiso para gestionar todas las entradas de seguridad en esta parte del sistema.
Leer	Habilita el permiso para ver los eventos genéricos en los clientes y el Management Client.
Editar	Habilita el permiso para editar las propiedades de los eventos genéricos en el Management Client.
Gestionar seguridad	Habilita el permiso para gestionar los permisos de seguridad en el Management Client para eventos genéricos.

Matrix

La funcionalidad disponible depende del sistema que esté utilizando. Vea la lista completa de características, que está disponible en la página de descripción del producto en el sitio web Milestone (https://www.milestonesys.com/solutions/platform/product-index/).

Permiso de seguridad	Descripción
Control total	Habilita el permiso para gestionar todas las entradas de seguridad en esta parte del sistema.
Leer	Habilita el permiso para seleccionar y enviar vídeo al destinatario Matrix desde los clientes.
Editar	Habilita el permiso para editar las propiedades de un Matrix en el Management Client.
Borrar	Habilita el permiso para eliminar un Matrix en el Management Client.

Permiso de seguridad	Descripción
Crear Matrix	Habilita el permiso para crear un nuevo Matrix en elManagement Client.
Gestionar seguridad	Habilita el permiso para gestionar los permisos de seguridad en el Management Client para todos los de Matrix.

Reglas

La funcionalidad disponible depende del sistema que esté utilizando. Vea la lista completa de características, que está disponible en la página de descripción del producto en el sitio web Milestone (https://www.milestonesys.com/solutions/platform/product-index/).

Permiso de seguridad	Descripción
Control total	Habilita el permiso para gestionar todas las entradas de seguridad en esta parte del sistema.
Leer	Habilita el permiso para ver las reglas existentes en el Management Client.
Editar	Habilita el permiso para editar las propiedades de las reglas y para definir el comportamiento de las mismas en el Management Client. También requiere que el usuario tenga permisos de lectura en todos los dispositivos que están afectados por la regla.
Borrar	Habilita el permiso para eliminar reglas del Management Client. También requiere que el usuario tenga permisos de lectura en todos los dispositivos que se vean afectados por la regla.
Crear regla	Habilita el permiso para crear nuevas reglas en el Management Client. También requiere que el usuario tenga permisos de lectura en todos los dispositivos que se vean afectados por la regla.
Gestionar seguridad	Habilita el permiso para gestionar los permisos de seguridad en el Management Client para todas las reglas.

Sitios

La funcionalidad disponible depende del sistema que esté utilizando. Vea la lista completa de características, que está disponible en la página de descripción del producto en el sitio web Milestone (https://www.milestonesys.com/solutions/platform/product-index/).

Permiso de seguridad	Descripción
Control total	Habilita el permiso para gestionar todas las entradas de seguridad en esta parte del sistema.
Leer	Habilita el permiso para ver otros sitios en el Management Client. Los sitios conectados se conectan mediante Milestone Federated Architecture. Para editar propiedades, necesita permisos de edición en el servidor de gestión en cada sitio.
Gestionar seguridad	Habilita el permiso para gestionar los permisos de seguridad en todos los sitios.

Monitor del sistema

La funcionalidad disponible depende del sistema que esté utilizando. Vea la lista completa de características, que está disponible en la página de descripción del producto en el sitio web Milestone (https://www.milestonesys.com/solutions/platform/product-index/).

Permiso de seguridad	Descripción
Control total	Habilita el permiso para gestionar todas las entradas de seguridad en esta parte del sistema.
Leer	Habilita el permiso para ver los monitores del sistema en XProtect Smart Client.

Permiso de seguridad	Descripción
Editar	Habilita el permiso para editar las propiedades de los monitores del sistema en el Management Client.
Gestionar seguridad	Habilita el permiso para gestionar los permisos de seguridad en el Management Client para todos los monitores del sistema.

Búsqueda de metadatos

La funcionalidad disponible depende del sistema que esté utilizando. Vea la lista completa de características, que está disponible en la página de descripción del producto en el sitio web Milestone (https://www.milestonesys.com/solutions/platform/product-index/).

Permiso de seguridad	Descripción
Control total	Habilita el permiso para gestionar todas las entradas de seguridad en esta parte del sistema.
Leer	La funcionalidad de **Uso de metadatos** en el Management Client y sus ajustes relacionados, pero no habilita el permiso para cambiar los ajustes.
Editar la configuración de búsqueda de metadatos	Habilita el permiso para habilitar o deshabilitar las categorías de búsqueda de metadatos, por ejemplo de personas o vehículos, en el Management Client.
Gestionar seguridad	Habilita el permiso para gestionar los permisos de seguridad de las búsquedas de metadatos.

Buscar

La funcionalidad disponible depende del sistema que esté utilizando. Vea la lista completa de características, que está disponible en la página de descripción del producto en el sitio web Milestone (https://www.milestonesys.com/solutions/platform/product-index/).

Permiso de seguridad	Descripción
Leer búsquedas públicas	Habilita el permiso para ver y abrir las búsquedas públicas guardadas en XProtect Smart Client.
Crear búsquedas públicas	Habilita el permiso para guardar las búsquedas recién configuradas como búsquedas públicas en XProtect Smart Client.
Editar búsquedas públicas	Habilita el permiso para editar los detalles o la configuración de las búsquedas públicas guardadas en XProtect Smart Client, por ejemplo el nombre, la descripción, las cámaras y las categorías de búsqueda.
Eliminar búsquedas públicas	Habilita el permiso para eliminar las búsquedas públicas guardadas.
Gestionar seguridad	Habilita el permiso para gestionar los permisos de seguridad en el Management Client para la búsqueda.

Alarmas

La funcionalidad disponible depende del sistema que esté utilizando. Vea la lista completa de características, que está disponible en la página de descripción del producto en el sitio web Milestone (https://www.milestonesys.com/solutions/platform/product-index/).

Permiso de seguridad	Descripción
Control total	Habilita el permiso para gestionar todas las entradas de seguridad en esta parte del sistema.
Gestión	Habilita el permiso para gestionar las alarmas en el Management Client. Por ejemplo, cambiar propiedades de alarmas y volver a delegar alarmas en otros usuarios, reconocer alarmas y cambiar el estado, por ejemplo, de Nueva a Asignada, de varias alarmas al mismo tiempo, definiciones de alarmas, sonidos de alarmas y ajustes de datos de alarmas. Solo cuando establece esto en permitido, aparece la pestaña **Alarmas y Eventos** en el cuadro de diálogo **Opciones**.
Editar	Habilita el permiso para ver las alarmas e imprimir los informes de alarma.
Desactivar alarmas	Habilita el permiso para desactivar las alarmas.
Recibir notificaciones	Habilita el permiso para recibir notificaciones sobre alarmas en clientes XProtect Mobile y XProtect Web Client.
Gestionar seguridad	Habilita el permiso para gestionar los permisos de seguridad de las alarmas.
Crear	Habilita el permiso para crear nuevas definiciones de alarma en el Management Client.

Registros de servidores

La funcionalidad disponible depende del sistema que esté utilizando. Vea la lista completa de características, que está disponible en la página de descripción del producto en el sitio web Milestone (https://www.milestonesys.com/solutions/platform/product-index/).

Permiso de seguridad	Descripción
Control total	Habilita el permiso para gestionar todas las entradas de seguridad en esta parte del sistema.
Leer entradas del registro del sistema	Habilita el permiso para ver las entradas del registro del sistema.
Leer entradas del registro de auditoría	Habilita el permiso para ver las entradas del registro de auditoría.
Leer entradas de registros activados por reglas	Habilita el permiso para ver las entradas de registro activadas por reglas.
Leer configuración del registro	Habilita el permiso para leer los ajustes del registro en **Herramientas** > **Opciones** > **Registros de servidor**.
Actualizar configuración de registro	Habilita el permiso para cambiar los ajustes del registro en **Herramientas** > **Opciones** > **Registros de servidor**.
Gestionar seguridad	Habilita el permiso para gestionar los permisos de seguridad de las alarmas.

Control de acceso

La funcionalidad disponible depende del sistema que esté utilizando. Vea la lista completa de características, que está disponible en la página de descripción del producto en el sitio web Milestone (https://www.milestonesys.com/solutions/platform/product-index/).

Permiso de seguridad	Descripción
Control total	Habilita el permiso para gestionar todas las entradas de seguridad en esta parte del sistema.
Editar	Habilita el permiso para editar las propiedades de los sistemas de Control de

Permiso de seguridad	Descripción
	acceso en el Management Client.
Usar control de acceso	Permite al usuario utilizar cualquier función relacionada con el control de acceso en los clientes.
Ver la lista de poseedores de tarjeta	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.
Gestionar seguridad	Habilita el permiso para gestionar los permisos de seguridad de todos los sistemas de Control de acceso.

LPR

Si su sistema funciona con XProtect LPR, especifique los siguientes permisos para el usuario:

Permiso de seguridad	Descripción
Control total	Habilita el permiso para gestionar todas las entradas de seguridad en esta parte del sistema.
Usar LPR	Habilita el permiso para utilizar cualquier característica relacionada con LPR en los clientes
Gestionar listas de coincidencias	Habilita el permiso para añadir, importar, modificar, exportar y eliminar listas de coincidencia de matrículas en el Management Client.
Leer listas de coincidencias	Habilita el permiso para ver las listas de coincidencia de matrículas.
Gestionar seguridad	Habilita el permiso para gestionar los permisos de seguridad en el Management Client para todas las definiciones de Transacción.

Fuentes de transacción

Permiso de seguridad	Descripción
Control total	Habilita el permiso para gestionar todas las entradas de seguridad en esta parte del sistema.
Leer	Habilita el permiso para ver las propiedades de las fuentes de transacción en el Management Client.
Editar	Habilita el permiso para editar las propiedades de las fuentes de transacción en el Management Client.
Borrar	Habilita el permiso para eliminar las fuentes de transacción en el Management Client.
Crear	Habilita el permiso para crear nuevas fuentes de transacción en el Management Client.
Gestionar seguridad	Habilita el permiso para gestionar los permisos de seguridad en el Management Client para todas las fuentes de Transacción.

Definición de la transacción

Permiso de seguridad	Descripción
Control total	Habilita el permiso para gestionar todas las entradas de seguridad en esta parte del sistema.
Leer	Habilita el permiso para ver las propiedades de las definiciones de las transacciones en el Management Client.
Editar	Habilita el permiso para editar las propiedades de las definiciones de las Transacciones en el Management Client.
Borrar	Habilita el permiso para eliminar las definiciones de las transacciones en el Management Client.
Crear	Habilita el permiso para crear nuevas definiciones de transacciones en el Management Client.
Gestionar seguridad	Habilita el permiso para gestionar los permisos de seguridad en el Management Client para todas las definiciones de Transacción.

MIP plug-ins

Mediante el MIP SDK, un proveedor externo puede desarrollar plug-ins personalizados para su sistema, por ejemplo, integración con sistemas de control externos o funcionalidades similares.

Pestaña Dispositivo (roles)

> La funcionalidad disponible depende del sistema que esté utilizando. Vea la lista completa de características, que está disponible en la página de descripción del producto en el sitio web Milestone (https://www.milestonesys.com/solutions/platform/product-index/).

La pestaña **Dispositivo** le permite especificar qué características los usuarios/grupos con el rol seleccionado pueden utilizar para cada dispositivo (por ejemplo, una cámara) o grupo de dispositivos en XProtect Smart Client.

Recuerde repetir para cada dispositivo. También puede seleccionar un grupo de dispositivos y especificar los permisos de los cometidos para todos los dispositivos del grupo de una sola vez.

Aún puede seleccionar o desactivar las casillas de verificación marcadas, pero tenga en cuenta que elección en este caso es aplicable a **todos** los dispositivos dentro del grupo de dispositivos. Alternativamente, seleccione los dispositivos individuales en el grupo de dispositivos para verificar exactamente a qué dispositivos se aplica el permiso correspondiente.

Permisos relacionados con la cámara

Especifique los siguientes permisos para los dispositivos de la cámara:

Nombre	Descripción
Leer	Las cámaras seleccionadas serán visibles en los clientes.
Ver en directo	Permite la visualización en directo de vídeo desde las cámaras seleccionadas en los clientes. Para XProtect Smart Client, requiere que el cometido haya recibido el permiso para ver la ficha de los clientes en **Directo**. Este permiso se concede como parte de los permisos de la aplicación. Especifique el perfil temporal o deje el valor predeterminado.
Ver directo restringido	Permite la visualización en directo de vídeo restringidos desde las cámaras seleccionadas en los clientes.

Nombre	Descripción
	Para XProtect Smart Client, requiere que el cometido haya recibido el permiso para ver la ficha de los clientes en **Directo**. Este permiso se concede como parte de los permisos de la aplicación. Especifique el perfil temporal o deje el valor predeterminado.
Reproducir > Dentro del perfil temporal	Permite reproducir vídeo grabado de las cámaras seleccionadas en los clientes. Especifique el perfil temporal o deje el valor predeterminado.
Reproducir > Limitar reproducción a	Permite reproducir vídeo grabado de las cámaras seleccionadas en los clientes. Especifique un límite de reproducción o no aplique restricciones.
Reproducción de grabaciones restringidas	Permite reproducir vídeo grabado restringido de la(s) cámara(s) seleccionada(s) en los clientes. Especifique el perfil temporal o deje el valor predeterminado.
Leer secuencias	Permite leer la información de la secuencia relacionada, por ejemplo, con el explorador de secuencias en los clientes.
Búsqueda avanzada	Permite al usuario utilizar la función de búsqueda inteligente en los clientes.
Exportar	Permite al usuario exportar grabaciones de los clientes.
Iniciar la grabación manual	Permite iniciar la grabación manual de vídeo desde las cámaras seleccionadas en los clientes.
Detener la grabación manual	Permite detener la grabación manual de vídeo desde las cámaras seleccionadas en los clientes.
Leer marcadores	Permite buscar y leer detalles de marcadores en los clientes.
Editar marcadores	Permite editar marcadores en los clientes.

Nombre	Descripción
Crear marcador	Permite añadir marcadores en los clientes.
Eliminar marcadores	Permite eliminar marcadores en los clientes.
Comandos AUX	Permite el uso de comandos auxiliares desde los clientes.
Crear y ampliar bloqueos de evidencias	Permite al usuario cliente: • Añadir la cámara a bloqueos de evidencias nuevos o existentes • Ampliar el tiempo de caducidad para los bloqueos de evidencias existentes • Ampliar el intervalo protegido para bloqueos de evidencias existentes Requiere permisos de usuario para todos los dispositivos incluidos en el bloqueo de evidencias.
Eliminar y reducir bloqueos de evidencias	Permite al usuario cliente: • Quitar la cámara de bloqueos de evidencias existentes • Eliminar bloqueos de evidencias existentes • Acortar el tiempo de vencimiento para los bloqueos de evidencias existentes • Acortar el intervalo protegido para bloqueos de evidencias existentes Requiere permisos de usuario para todos los dispositivos incluidos en el bloqueo de evidencias.
Leer bloqueo de evidencias	Permite al usuario cliente buscar y leer detalles de bloqueos de evidencias.
Crear y ampliar restricciones en vivo y para la reproducción	Permite al usuario cliente: • Crear una restricción en directo en la cámara • Crear una restricción de reproducción en las grabaciones de cámara

Nombre	Descripción
	• Añadir una cámara nueva a una restricción en directo o de reproducción • Prolongar el periodo de restricción de las grabaciones de la cámara Requiere permisos de usuario para todos los dispositivos incluidos en la restricción.
Leer restricciones en directo y para la reproducción	Permite al usuario cliente: • Ver una lista de las restricciones en directo y de reproducción existentes en la cámara. • Filtrar y buscar en la lista de las restricciones en directo y de reproducción en la cámara.
Eliminar y reducir restricciones en directo y para la reproducción	Permite al usuario cliente: • Eliminar una restricción en directo de la cámara • Eliminar una restricción de reproducción en las grabaciones de cámara • Reducir el periodo de restricción de las grabaciones de cámara • Cambiar los ajustes de la restricción en directo o de reproducción Requiere permisos de usuario para todos los dispositivos incluidos en la restricción.

Permisos relacionados con el micrófono

Especificar los siguientes permisos para los dispositivos de micrófono:

Nombre	Descripción
Leer	Los micrófonos seleccionados serán visibles en los clientes.
Escucha en directo	Permite escuchar audio en directo desde los micrófonos seleccionados en los

Nombre	Descripción
	clientes. Para XProtect Smart Client, requiere que el cometido haya recibido el permiso para ver la ficha de los clientes en **Directo**. Este permiso se concede como parte de los permisos de la aplicación. Especifique el perfil temporal o deje el valor predeterminado.
Escuchar audio en directo restringido	Permite escuchar audio en directo restringido desde el/los micrófono(s) seleccionado(s) en los clientes. Para XProtect Smart Client, requiere que el cometido haya recibido el permiso para ver la ficha de los clientes en **Directo**. Este permiso se concede como parte de los permisos de la aplicación. Especifique el perfil temporal o deje el valor predeterminado.
Reproducir > Dentro del perfil temporal	Permite reproducir audio grabado desde los micrófonos seleccionados en los clientes. Especifique el perfil temporal o deje el valor predeterminado.
Reproducir > Limitar reproducción a	Permite reproducir audio grabado desde los micrófonos seleccionados en los clientes. Especifique un límite de reproducción o no aplique restricciones.
Reproducción de grabaciones restringidas	Permite reproducir audio grabado restringido desde el/los micrófono(s) seleccionado(s) en los clientes. Especifique el perfil temporal o deje el valor predeterminado.
Leer secuencias	Permite leer la información de la secuencia relacionada, por ejemplo, con el explorador de secuencias en los clientes.
Exportar	Permite al usuario exportar grabaciones de los clientes.
Iniciar la grabación manual	Permite iniciar la grabación manual de audio desde los micrófonos seleccionados en los clientes.
Detener la grabación manual	Permite detener la grabación manual de audio desde los micrófonos seleccionados en los clientes.

Nombre	Descripción
Leer marcadores	Permite buscar y leer detalles de marcadores en los clientes.
Editar marcadores	Permite editar marcadores en los clientes.
Crear marcador	Permite añadir marcadores en los clientes.
Eliminar marcadores	Permite eliminar marcadores en los clientes.
Crear y ampliar bloqueos de evidencias	Permite al usuario cliente: • Añadir el micrófono a bloqueos de evidencias nuevos o existentes • Ampliar el tiempo de caducidad para los bloqueos de evidencias existentes • Ampliar el intervalo protegido para bloqueos de evidencias existentes  Requiere permisos de usuario para todos los dispositivos incluidos en el bloqueo de evidencias.
Eliminar y reducir bloqueos de evidencias	Permite al usuario cliente: • Quitar el micrófono de bloqueos de evidencias existentes • Eliminar bloqueos de evidencias existentes • Acortar el tiempo de vencimiento para los bloqueos de evidencias existentes • Acortar el intervalo protegido para bloqueos de evidencias existentes  Requiere permisos de usuario para todos los dispositivos incluidos en el bloqueo de evidencias.
Leer bloqueo de evidencias	Permite al usuario cliente buscar y leer detalles de bloqueos de evidencias.
Crear y ampliar	Permite al usuario cliente:

Nombre	Descripción
restricciones en vivo y para la reproducción	• Crear una restricción en directo en el micrófono • Crear una restricción de reproducción en las grabaciones de audio • Añadir un nuevo micrófono a una restricción en directo o de reproducción • Prolongar el periodo de restricción de las grabaciones de audio  Requiere permisos de usuario para todos los dispositivos incluidos en la restricción.
Leer restricciones en directo y para la reproducción	Permite al usuario cliente: • Ver una lista de las restricciones en directo y de reproducción existentes en el micrófono • Filtrar y buscar en la lista de las restricciones en directo y de reproducción en el micrófono
Eliminar y reducir restricciones en directo y para la reproducción	Permite al usuario cliente: • Eliminar una restricción en directo en el micrófono • Eliminar una restricción de reproducción en las grabaciones de audio • Reducir el periodo de restricción de las grabaciones de audio • Cambiar los ajustes de la restricción en directo o de reproducción  Requiere permisos de usuario para todos los dispositivos incluidos en la restricción.

Permisos relacionados con los altavoces

Especificar los siguientes permisos para los dispositivos de altavoces:

Nombre	Descripción
Leer	Los altavoces seleccionados son visibles en los clientes.
Escucha en directo	Permite escuchar audio en directo desde los altavoces seleccionados en los clientes. Para XProtect Smart Client, requiere que el cometido haya recibido el permiso para ver la ficha de los clientes en **Directo**. Este permiso se concede como parte de los permisos de la aplicación. Especifique el perfil temporal o deje el valor predeterminado.
Escuchar audio en directo restringido	Permite escuchar vídeo en directo restringido desde el/los altavoz/ces seleccionado(s) en los clientes. Para XProtect Smart Client, requiere que el cometido haya recibido el permiso para ver la ficha de los clientes en **Directo**. Este permiso se concede como parte de los permisos de la aplicación. Especifique el perfil temporal o deje el valor predeterminado.
Reproducir > Dentro del perfil temporal	Permite reproducir audio grabado desde los altavoces seleccionados en los clientes. Especifique el perfil temporal o deje el valor predeterminado.
Reproducir > Limitar reproducción a	Permite reproducir audio grabado desde los altavoces seleccionados en los clientes. Especifique un límite de reproducción o no aplique restricciones.
Reproducción de grabaciones restringidas	Permite reproducir audio grabado restringido desde el/los altavoz/ces seleccionado(s) en los clientes. Especifique el perfil temporal o deje el valor predeterminado.
Leer secuencias	Permite leer la información de la secuencia relacionada, por ejemplo, con el explorador de secuencias en los clientes.
Exportar	Permite al usuario exportar grabaciones de los clientes.
Iniciar la grabación manual	Permite iniciar la grabación manual de audio desde los altavoces seleccionados en los clientes.

Nombre	Descripción
Detener la grabación manual	Permite detener la grabación manual de audio desde los altavoces seleccionados en los clientes.
Leer marcadores	Permite buscar y leer detalles de marcadores en los clientes.
Editar marcadores	Permite editar marcadores en los clientes.
Crear marcador	Permite añadir marcadores en los clientes.
Eliminar marcadores	Permite eliminar marcadores en los clientes.
Crear y ampliar bloqueos de evidencias	Permite al usuario cliente: • Añadir el altavoz a bloqueos de evidencias nuevos o existentes • Ampliar el tiempo de caducidad para los bloqueos de evidencias existentes • Ampliar el intervalo protegido para bloqueos de evidencias existentes Requiere permisos de usuario para todos los dispositivos incluidos en el bloqueo de evidencias.
Eliminar y reducir bloqueos de evidencias	Permite al usuario cliente: • Quitar el altavoz de los bloqueos de evidencias existentes • Eliminar bloqueos de evidencias existentes • Acortar el tiempo de vencimiento para los bloqueos de evidencias existentes • Acortar el intervalo protegido para bloqueos de evidencias existentes Requiere permisos de usuario para todos los dispositivos incluidos en el bloqueo de evidencias.

Nombre	Descripción
Leer bloqueo de evidencias	Permite al usuario cliente buscar y leer detalles de bloqueos de evidencias.
Crear y ampliar restricciones en vivo y para la reproducción	Permite al usuario cliente: • Crear una restricción en directo en los altavoces • Crear una restricción de reproducción en las grabaciones de audio • Añadir un nuevo micrófono a una restricción en directo o de reproducción • Prolongar el periodo de restricción de las grabaciones de audio  Requiere permisos de usuario para todos los dispositivos incluidos en la restricción.
Leer restricciones en directo y para la reproducción	Permite al usuario cliente: • Ver una lista de las restricciones en directo y de reproducción existentes en los altavoces • Filtrar y buscar en la lista de las restricciones en directo y de reproducción en los altavoces
Eliminar y reducir restricciones en directo y para la reproducción	Permite al usuario cliente: • Eliminar una restricción en directo en los altavoces • Eliminar una restricción de reproducción en las grabaciones de audio • Reducir el periodo de restricción de las grabaciones de audio • Cambiar los ajustes de la restricción en directo o de reproducción  Requiere permisos de usuario para todos los dispositivos incluidos en la restricción.

Permisos relacionados con los metadatos

Especificar los siguientes permisos para los dispositivos de metadatos:

Nombre	Descripción
Leer	Habilita el permiso para ver los dispositivos de metadatos y recuperar datos de ellos en los clientes.
Editar	Habilita el permiso para editar las propiedades de los metadatos. También permite a los usuarios habilitar o deshabilitar dispositivos de metadatos en el Management Client y mediante MIP SDK.
Ver en directo	Habilita el permiso para ver los metadatos de las cámaras de los clientes en directo. Para XProtect Smart Client, requiere que el cometido haya recibido el permiso para ver la ficha de los clientes en **Directo**. Este permiso se concede como parte de los permisos de la aplicación.
Ver restricción en vivo	Habilita el permiso para ver los metadatos restringidos en directo de las cámaras de los clientes. Para XProtect Smart Client, requiere que el cometido haya recibido el permiso para ver la ficha de los clientes en **Directo**. Este permiso se concede como parte de los permisos de la aplicación.
Reproducción	Habilita el permiso para reproducir los datos grabados de los dispositivos de metadatos en los clientes.
Reproducción de grabaciones restringidas	Habilita el permiso para reproducir los datos grabados de los dispositivos de metadatos restringidos en los clientes.
Leer secuencias	Habilita el permiso para utilizar la función de Secuencias durante la exploración de los datos grabados de los dispositivos de metadatos en los clientes.
Exportar	Habilita el permiso para exportar el audio grabado de los dispositivos de metadatos en los clientes.
Crear y ampliar bloqueos de evidencias	Habilita el permiso para crear y ampliar los bloqueos de evidencia en los metadatos de los clientes.

Nombre	Descripción
Leer bloqueo de evidencias	Habilita el permiso para ver los bloqueos de evidencia en los metadatos de los clientes.
Eliminar y reducir bloqueos de evidencias	Habilita el permiso para eliminar o reducir los bloqueos de evidencia en los metadatos de los clientes.
Iniciar la grabación manual	Habilita el permiso para iniciar la grabación manual de metadatos en los clientes.
Detener la grabación manual	Habilita el permiso para detener la grabación manual de metadatos en los clientes.
Crear y ampliar restricciones en vivo y para la reproducción	Permite al usuario cliente: • Crear una restricción en directo en los dispositivos de los metadatos • Crear una restricción de reproducción en el dispositivo de los metadatos • Añadir nuevos metadatos a una restricción en directo o de reproducción • Prolongar el periodo de restricción de los dispositivos de los metadatos Requiere permisos de usuario para todos los dispositivos incluidos en la restricción.
Leer restricciones en directo y para la reproducción	Permite al usuario cliente: • Ver una lista de las restricciones en directo y de reproducción existentes en los dispositivos de los metadatos • Filtrar y buscar en la lista de las restricciones en directo y de reproducción en los dispositivos de los metadatos

Nombre	Descripción
Eliminar y reducir restricciones en directo y para la reproducción	Permite al usuario cliente: • Eliminar una restricción en directo en los dispositivos de los metadatos • Eliminar una restricción de reproducción en los dispositivos de los metadatos • Reducir el periodo de restricción de los dispositivos de los metadatos • Cambiar los ajustes de la restricción en directo o de reproducción  Requiere permisos de usuario para todos los dispositivos incluidos en la restricción.

Permisos relacionados con la entrada

Especifique los siguientes permisos para los dispositivos de entrada:

Nombre	Descripción
Leer	Las entradas seleccionadas serán visibles en los clientes.

Permisos relacionados con la salida

Especificar los siguientes permisos para los dispositivos de salida:

Nombre	Descripción
Leer	Las salidas seleccionadas serán visibles en los clientes. Si es visible, la salida será detectable en una lista en los clientes.
Activar	Las salidas seleccionadas se pueden activar desde el Management Client y los clientes. Especifique el perfil temporal o deje el valor predeterminado.

Pestaña PTZ (roles)

Puede configurar los permisos para las cámaras pan-tilt-zoom (PTZ) en la pestaña **PTZ**. Puede especificar las funciones que los usuarios/grupos pueden usar en los clientes. Puede seleccionar cámaras PTZ individuales o grupos de dispositivos que contengan cámaras PTZ.

Especificar los siguientes permisos para PTZ:

Nombre	Descripción
PTZ manual	Determina si el rol seleccionado puede usar funciones de PTZ y pausar una vigilancia en la cámara seleccionada. Especifique un perfil temporal, seleccione **Siempre** o deje el valor predeterminado que sigue el perfil temporal predeterminado definido en la pestaña **Información** para ese rol.
Activar valores preestablecidos PTZ o perfiles de patrulla	Determina si el rol seleccionado puede mover la cámara seleccionada a posiciones preestablecidas, iniciar y detener perfiles de vigilancia y pausar una vigilancia. Especifique un perfil temporal, seleccione **Siempre** o deje el valor predeterminado que sigue el perfil temporal predeterminado definido en la pestaña **Información** para ese rol. Para permitir que este cometido utilice otras funciones PTZ en la cámara, habilite el permiso **PTZ manual**.
Prioridad de PTZ	Determina la prioridad de las cámaras PTZ. Cuando varios usuarios en un sistema de vigilancia quieren controlar el sistema PTZ al mismo tiempo, pueden surgir conflictos. Puede evitar esta situación especificando una prioridad para el uso de cámaras PTZ seleccionadas por usuarios/grupos con el grupo seleccionado. Especifique una prioridad de 1 a 32 000, donde 1 es la prioridad más baja. La prioridad predeterminada es 3000. El rol con el número de prioridad más alta es el que puede controlar las cámaras PTZ.
Gestionar valores preestablecidos PTZ o perfiles de patrulla	Determina el permiso para añadir, editar y eliminar valores preestablecidos PTZ y perfiles de patrulla en la cámara seleccionada tanto en el Management Client y en el XProtect Smart Client. Para permitir que este cometido utilice otras funciones PTZ en la

Nombre	Descripción
	cámara, habilite el permiso **PTZ manual**.
Bloquear/Desbloquear valores preestablecidos PTZ	Determina si el rol puede bloquear y desbloquear posiciones preestablecidas para la cámara seleccionada.
Reservar sesiones PTZ	Determina el permiso para poner la cámara seleccionada en modo de sesión PTZ reservada. En una sesión PTZ reservada otros usuarios o sistemas de vigilancia con una mayor prioridad de PTZ no pueden asumir el control. Para permitir que este cometido utilice otras funciones PTZ en la cámara, habilite el permiso **PTZ manual**.
Liberar sesione PTZ	Determina si el rol seleccionado puede liberar sesiones PTZ de otros usuarios desde Management Client. Siempre puede liberar sus propias sesiones de PTZ - sin este permiso.

Pestaña Habla (roles)

Relevante solo si utiliza altavoces en su sistema. Especifique los siguientes permisos para los altavoces:

Nombre	Descripción
Hablar	Determine si se debe permitir a los usuarios hablar por los altavoces seleccionados. Especifique el perfil temporal o deje el valor predeterminado.
Prioridad de habla	Cuando varios clientes quieren hablar por el mismo altavoz al mismo tiempo, pueden surgir conflictos. Resuelva el problema especificando una prioridad para el uso de altavoces seleccionados por usuarios/grupos con el rol seleccionado. Especifique una prioridad desde **Muy baja** a **Muy alta**. El rol con la prioridad más alta tiene permiso para usar el altavoz antes que otros roles. En el caso de que dos usuarios con el mismo rol quieran hablar al mismo tiempo, se aplica el principio de que la prioridad la tiene el primero que llegue.

Pestaña Grabaciones remotas (roles)

Especificar los siguientes permisos para las grabaciones remotas:

Nombre	Descripción
Recuperar grabaciones a distancia	Habilita el permiso para recuperar las grabaciones en los clientes desde las cámaras, los micrófonos, los altavoces y los dispositivos de metadatos en los sitios remotos o desde los almacenamientos de borde en las cámaras.

Smart Wall pestaña (funciones)

A través de los cometidos, puede conceder a sus usuarios clientes permisos relacionados con Smart Wall:

Nombre	Descripción
Leer	Permite a los usuarios ver lo seleccionado Smart Wall en XProtect Smart Client.
Editar	Permite a los usuarios editar la Smart Wall seleccionada en el Management Client.
Borrar	Permite a los usuarios eliminar el Smart Wall seleccionado en el Management Client.
Operar	Permite a los usuarios aplicar distribuciones en la Smart Wall seleccionada en XProtect Smart Client y activar valores preestablecidos.
Reproducción	Permite a los usuarios reproducir los datos grabados de la memoria seleccionada Smart Wall en XProtect Smart Client.

Pestaña Evento externo (roles)

Especifique los siguientes permisos de eventos externos:

Nombre	Descripción
Leer	Permite a los usuarios buscar y ver el evento del sistema externo seleccionado en los

Nombre	Descripción
	clientes y en Management Client.
Editar	Permite a los usuarios editar el evento del sistema externo seleccionado en Management Client.
Borrar	Permite a los usuarios eliminar el evento del sistema externo seleccionado en Management Client.
Activador	Permite a los usuarios desencadenar el evento del sistema externo seleccionado en los clientes.

Pestaña Grupo de vistas (roles)

En la pestaña **Grupo de vistas**, especifique qué grupos de vistas pueden usar en los clientes los usuarios y los grupos con el rol seleccionado.

Especificar los siguientes permisos para los grupos de vistas:

Nombre	Descripción
Leer	Habilita el permiso para ver los Grupos de vista en los clientes y en el Management Client. Los grupos de vistas se crean en el Management Client.
Editar	Habilita el permiso para editar las propiedades de los Grupos de vista en el Management Client.
Borrar	Habilita el permiso para eliminar Grupos de vista en el Management Client.
Operar	Habilita el permiso para utilizar los grupos de vistas en XProtect Smart Client, es decir, para crear y eliminar subgrupos y vistas.

Pestaña Servidores (roles)

Especificar los permisos de los cometidos en la pestaña **Servidores** solo es relevante si su sistema funciona en una configuración Milestone Federated Architecture.

Nombre	Descripción
Sitios	Habilita el permiso para ver el sitio seleccionado en el Management Client. Los sitios conectados se conectan mediante Milestone Federated Architecture. Para editar propiedades, necesita permisos de edición en el servidor de gestión en cada sitio.

Consultar Configuración de Milestone Federated Architecture en la página 95 para obtener más información.

Matrix pestaña (funciones)

Si ha configurado los destinatarios Matrix en su sistema, puede configurar los permisos de los cometidos de Matrix. Desde un cliente, puede enviar vídeo a destinatarios de Matrix seleccionados. Seleccione los usuarios que pueden recibir esto en la pestaña Matrix.

Los siguientes permisos están disponibles:

Nombre	Descripción
Leer	Determine si los usuarios y los grupos con el rol seleccionado pueden seleccionar y enviar vídeo al destinatario de Matrix desde los clientes.

Pestaña Alarmas (roles)

Si utiliza las alarmas en la configuración de su sistema para proporcionar una visión general y un control centralizados de su instalación (incluyendo cualquier otro servidor XProtect), puede utilizar la pestaña **Alarmas** para especificar los permisos de alarma para los usuarios y grupos con el cometido seleccionado que deben tener, por ejemplo, cómo gestionar las alarmas en los clientes.

Especifique los siguientes permisos para las alarmas:

Nombre	Descripción
Gestión	Habilita el permiso para gestionar las alarmas, por ejemplo, cambiando las prioridades de las alarmas y redelegando las alarmas a otros usuarios, reconociendo las alarmas y cambiando el estado, por ejemplo, de **Nuevo** a **Asignado**, de varias

Nombre	Descripción
	alarmas al mismo tiempo.
Vista	Habilita el permiso para ver las alarmas e imprimir los informes de alarma.
Desactivar alarmas	Habilita el permiso para desactivar las alarmas.
Recibir notificaciones	Habilita el permiso para recibir notificaciones sobre alarmas en clientes XProtect Mobile y XProtect Web Client.

Pestaña Control de acceso (roles)

Cuando se añaden o editan usuarios básicos, usuarios o grupos de Windows, especifique los justes de control de acceso:

Nombre	Descripción
Usar control de acceso	Permite al usuario utilizar cualquier función relacionada con el control de acceso en los clientes.
Ver la lista de poseedores de tarjeta	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.

Pestaña LPR (roles)

Si su sistema funciona con XProtect LPR, especifique los siguientes permisos para los usuarios:

Nombre	Descripción
Usar LPR	Habilita el permiso para utilizar cualquier característica relacionada con LPR en los clientes.
Gestionar listas de coincidencias	Habilita el permiso para añadir, importar, modificar, exportar y eliminar listas de coincidencia de matrículas en el Management Client.
Leer listas de coincidencias	Habilita el permiso para ver las listas de coincidencia de matrículas.

Pestaña Inicdentes (roles)

Si tiene XProtect Incident Manager, puede especificar los permisos siguientes para sus cometidos.

Para dar a un cometido de administrador de Management Client los permisos para gestionar o visualizar propiedades de incidentes, seleccione el nodo **Propiedades de incidentes**.

Para dar a un operador de XProtect Smart Client permiso para ver las propiedades del incidente definidas, seleccione **Propiedades del incidente** y conceda el permiso **Ver**. Para dar permisos generales para gestionar o visualizar proyectos de incidentes, seleccione el nodo **Proyecto de incidente**. Expanda el nodo **Proyecto de incidente** y seleccione uno o más subnodos para dar permisos para estas características o capacidades específicas adicionales.

Nombre	Descripción
Gestión	Permiso para gestionar (ver, crear, editar y borrar) ajustes y propiedades relacionados con una característica o ver un elemento de la interfaz de usuario representado por el nodo seleccionado en Management Client o XProtect Smart Client.
Vista	Permiso para ver (pero no crear, editar y borrar) ajustes y propiedades relacionados con una característica, vista, propiedades del incidente definidas, o ver un elemento de la interfaz de usuario representado por el nodo seleccionado en Management Client o XProtect Smart Client.

MIP pestaña (funciones)

Mediante el MIP SDK, un proveedor externo puede desarrollar plug-ins personalizados para su sistema, por ejemplo, integración con sistemas de control externos o funcionalidades similares.

Los ajustes que cambie dependen del plug-in real. Busque los ajustes personalizados para los plug-in en la pestaña **MIP**.

Usuario básico (nodo Seguridad)

Existen dos tipos de cuentas de usuario de Milestone XProtect VMS: Usuarios básicos y usuarios de Windows.

Los usuarios básicos son cuentas de usuario que crea en Milestone XProtect VMS. Se trata de una cuenta de usuario del sistema dedicada con un nombre de usuario básico y una contraseña de autenticación para cada usuario individual.

Los usuarios de Windows son cuentas de usuario que añades a través de Active Directory de Microsoft.

Hay algunas diferencias básicas entre usuarios básicos y usuarios de Windows:

- Los usuarios básicos se autentican mediante una combinación de nombre de usuario y contraseña y son específicos de un sitio/sistema. Tenga en cuenta que aunque un usuario básico creado en un sitio federado tenga el mismo nombre y contraseña que un usuario básico de otro sitio federado, el usuario básico solo tiene acceso al sitio en el que se ha creado.
- Los usuarios de Windows se autentifican mediante su inicio de sesión en Windows y son específicos de una máquina.

Nodo Panel del sistema

Nodo Panel del sistema

En el nodo **Panel de control del sistema**, encuentra una funcionalidad distinta para monitorizar su sistema y sus distintos componentes del sistema.

Nombre	Descripción
Tarea actual	Obtenga una descripción general de tareas en curso en un servidor de grabación seleccionado.
Monitor del sistema	Monitorice el estado de sus servidores y cámaras mediante parámetros que defina.
Umbrales del monitor del sistema	Establezca los valores de umbral para parámetros monitorizados en los mosaicos de servidores y monitores utilizados en Monitor del sistema.

Nombre	Descripción
Bloqueo de evidencias	Obtenga una descripción general de todos los datos protegidos en el sistema.
Informes de configuración	Imprima un informe con su configuración del sistema. Puede decidir qué incluir en el informe.

Tareas actuales (nodo Panel de control del sistema)

La ventana **Tareas actuales** muestra una descripción general de tareas en curso en un servidor de grabación seleccionado. Si ha iniciado una tarea que tarda mucho tiempo y se ejecuta en segundo plano, puede abrir la ventana **Tareas actuales** para ver cómo progresa la tarea. Unos pocos ejemplos de tareas de larga duración iniciadas por el usuario son actualizaciones de firmware y movimiento de hardware. Puede ver información sobre la hora de inicio de las tareas, la hora de finalización estimada y el progreso.

La información que se muestra en la ventana **Tareas actuales** no se actualiza de forma dinámica, sino que es una instantánea de las tareas actuales desde el momento en que abrió la ventana. Si ha tenido abierta la ventana durante algún tiempo, actualice la información seleccionando el botón **Actualizar** en la esquina inferior derecha de la ventana.

Monitor del sistema (nodo Panel del sistema)

La funcionalidad **Monitor del sistema** le proporciona una rápida descripción visual del estado actual de los servidores y las cámaras de su sistema.

Ventana del panel del monitor del sistema

Mosaicos

La parte superior de la ventana **Panel del monitor del sistema** muestra mosaicos de colores que representan el estado del hardware de servidores y del hardware de cámaras del sistema.

Los mosaicos cambian de estado y, por tanto, de color, en función de los valores umbrales establecidos en el nodo **Umbrales de los monitores del sistema**. Para obtener más información, consulte Umbrales del monitor del sistema (nodo Panel del sistema) en la página 597. Defina los umbrales, de modo que los colores de los mosaicos signifiquen lo siguiente:

Color del mosaico	Descripción
Verde	Estado **Normal**. Todo funciona con normalidad.
Amarillo	Estado de **Alerta**. Uno o más parámetros de monitorización están por encima del valor umbral para el estado **Normal**.
Rojo	Estado **Crítico**. Uno o más parámetros de monitorización están por encima del valor umbral para el estado **Normal** y **Advertencia**.

Lista de hardware con parámetros de monitorización

Si hace clic en un mosaico, puede ver el estado de cada parámetro de monitorización para cada hardware representado por el mosaico en la parte inferior de la ventana **Panel del monitor del sistema**.

Ejemplo: Los parámetros de monitorización de FPS EN DIRECTO de la cámara han alcanzado el estado Advertencia.

Personalizar ventana del panel de control

Seleccione **Personalizar** en la esquina superior derecha de la ventana para abrir la ventana **Personalizar panel**.

En la ventana **Personalizar panel**, puede seleccionar qué mosaico crear, editar o eliminar. Al crear o editar mosaicos, puede seleccionar qué hardware y qué parámetros de monitorización quiere monitorizas en el mosaico.

Ventana Detalles

Si selecciona un mosaico y, a continuación, desde la lista de hardware con parámetros de monitorización, selecciona el botón **Detalles** a la derecha de la cámara o el servidor, puede -dependiendo del hardware seleccionado- ver información del sistema y crear informes sobre:

Hardware	Información
Servidor de gestión	Muestra datos sobre: • Uso de la CPU

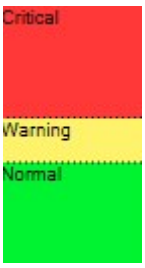
Hardware	Información
	• Memoria disponible Seleccione **Historial** para ver los estados históricos de su hardware y crear un informe sobre los datos anteriores.
Servidor(es) de grabación	Muestra datos sobre: • % uso de CPU • Memoria disponible • Discos • Almacenamiento • Red • Cámaras Seleccione **Historial** para ver los estados históricos de su hardware y crear un informe sobre los datos anteriores.
Servidores de grabación de failover	Muestra datos sobre: • % uso de CPU • Memoria disponible • Servidores de grabación monitorizados Seleccione **Historial** para ver los estados históricos de su hardware y crear un informe sobre los datos anteriores.
Servidores de registro, servidores de eventos y más	Muestra datos sobre • % uso de CPU • Memoria disponible Seleccione **Historial** para ver los estados históricos de su hardware y crear un informe sobre los datos anteriores.
Cámaras	Muestra datos sobre: • Almacenamiento

Hardware	Información
	• Espacio utilizado • FPS en directo (Predeterminado) • Grabando FPS • Formato de vídeo en directo • Formato de vídeo de grabación • Datos de medios recibidos (Kbit/s) • Memoria disponible Seleccione el nombre de la cámara para ver su historial de estados y crear un informe sobre: • Datos recibidos de la cámara • Uso del disco de la cámara

Si accede a los detalles del monitor del sistema desde el sistema operativo de un servidor, puede recibir un mensaje sobre **Configuración de seguridad mejorada de Internet Explorer**. Siga las instrucciones para añadir la página **Monitor del sistema** a la **Zona de sitios de confianza** antes de proceder.

Umbrales del monitor del sistema (nodo Panel del sistema)

Los umbrales del monitor del sistema le permite definir y ajustar los umbrales cuando los mosaicos en el **Panel de control del monitor del sistema** debe indicar visualmente que el hardware de su sistema cambia de estado. Por ejemplo, cuando el uso de la CPI de un servidor cambia de un estado normal (verde) a un estado de advertencia (amarillo) o de un estado de advertencia (amarillo) a un estado crítico (rojo).



Ejemplo de umbrales entre los tres estados

Puede cambiar umbrales para servidores, cámaras, discos y almacenamiento, y todos los umbrales tienen algunos botones y ajustes comunes.

Elementos comunes de la interfaz de usuario

Botones y ajustes	Descripción	Unidad
Intervalo de cálculo	A menudo hay breves interrupciones en la conexión a su distinto hardware. Si especifica un intervalo de cálculo de 0 segundos, todas estas breves interrupciones activarán alertas sobre cambios en el estado del hardware. Por lo tanto, defina un intervalo de cálculo de cierta longitud. Si define un cálculo interno de un (1) minuto, significa que solo recibe alertas si el valor promedio para el minuto entero excede el umbral. Con el ajuste del intervalo de cálculo correcto, no recibirá alertas falsas positivas, sino solo alertas sobre problemas sostenidos con, por ejemplo, uso de la CPI o consumo de memoria. Para cambiar los valores de los intervalos de cálculo consulte Editar umbrales para cuando los estados del hardware deben cambiar en la página 305.	seg.
Avanzados	Si selecciona el botón **Avanzada**, puede definir umbrales e intervalos de cálculo para servidores, cámaras, discs y almacenamientos individuales. Para obtener más información, consulte a continuación.	-
Crear regla	Puede combinar eventos desde el **Monitor del sistema** y reglas para desencadenar acciones, por ejemplo, cuando el uso de la CPU del servidor es crítica, o cuando un disco se está quedando sin espacio libre. Si desea más información, consulte Reglas y eventos (explicación) en la página 79 y Añadir reglas en la página 280.	-

Umbrales del servidor

Umbral	Descripción	Unidad
% uso de CPU	Umbrales para el uso de la CPU en los servidores que monitoriza.	%
Memoria disponible	Umbrales para la RAM en uso en los servidores de monitoriza.	MB
Decodificación de NVIDIA	Umbrales para el uso de decodificación de NVIDIA en los servidores que monitoriza.	%
Memoria de NVIDIA	Umbrales para la RAM NVIDIA en uso en los servidores que monitoriza.	%
Procesamiento de NVIDIA	Umbrales para el uso de renderización de NVIDIA en los servidores que monitoriza.	%

Umbrales de la cámara

Umbral	Descripción	Unidad
FPS en directo	Umbrales para los FPS de las cámaras en uso cuando se muestra vídeo en directo en las cámaras que monitoriza.	%
Grabando FPS	Umbrales para los FPS de las cámaras en uso cuando el sistema está grabando vídeo en las cámaras que monitoriza.	%
Espacio utilizado	Umbrales para el espacio utilizado por las cámaras que monitoriza.	GB

Umbrales del disco

Umbral	Descripción	Unidad
Espacio libre	Umbrales para el espacio disponible en los discos que monitoriza.	GB

Umbrales de almacenamiento

Umbral	Descripción	Unidad
Periodo de retención	Umbral que muestra una predicción para cuando se queda sin espacio de almacenamiento. El estado que se muestra se basa en la configuración de su sistema y se actualizada dos veces al día.	Días

Bloqueo de evidencias (nodo Panel de control del sistema)

Bloqueo de evidencias en el nodo **Panel de control del sistema** muestra una descripción general de todos los datos protegidos en el sistema de vigilancia actual.

Los siguientes metadatos están disponibles para todos los bloqueos de evidencias:

- Fecha de inicio y fin para los datos protegidos
- El usuario que bloqueó la evidencia
- Cuando la evidencia ya no está bloqueada
- Dónde se almacenan los datos
- El tamaño de cada bloqueo de evidencias

Toda la información que se muestra en la ventana **Bloqueo de evidencias** son instantáneas. Pulse F5 para actualizar.

Informes de configuración (nodo Panel de control del sistema)

Al instalar y configurar el sistema VMS, se hacen muchas elecciones y es posible que tenga que documentarlas. Con el tiempo también es difícil recordar todos los ajustes que se han cambiado desde la instalación y la configuración inicial, o solo durante el último par de meses. Por este motivo es posible imprimir un informe con todas sus opciones de configuración.

Los siguientes ajustes están disponibles al crear e imprimir informes de configuración:

Nombre	Descripción
Informes	Una lista de elementos que es posible incluir en un informe de configuración.
Selec. todo	Añade todos los elementos de la lista **Informes** al informe de configuración.

Nombre	Descripción
Limpiar todo	Quita todos los elementos de la lista **Informes** del informe de configuración.
Portada	Personalice la portada del informe.
Formateado	Dé formato al informe.
Excluir datos sensibles	Quita datos personales, como nombres de usuarios, direcciones de correo electrónico y otros tipos de datos sensibles del informe de configuración y hace que cumpla con el RGPD. La información sobre el propietario de la licencia siempre se excluye del informe.
Exportar	Seleccione una ubicación segura para el informe y créelo como un PDF.

Nodo Registros del servidor

Nodo Registros del servidor

Registros del sistema (pestaña)

Cada fila en un registro representa una entrada del registro. Una entrada de registro contiene una serie de campos de información:

Nombre	Descripción
Nivel de registro	Información, advertencia o error.
Hora local	Con la marca de tiempo en la hora local del servidor de su sistema.
Texto del mensaje	El número de identificación para el incidente registrado.
Categoría	El tipo de incidente registrado.

Nombre	Descripción
Tipo de fuente	El tipo de equipo en el que se produjo el incidente registrado, por ejemplo, servidor o dispositivo.
Nombre de la fuente	El nombre del equipo en el que se produjo el incidente registrado.
Tipo de evento	El tipo de evento representado por el incidente registrado.

Registros de auditoría (pestaña)

Cada fila en un registro representa una entrada del registro. Una entrada de registro contiene una serie de campos de información:

Nombre	Descripción
Hora local	Con la marca de tiempo en la hora local del servidor de su sistema.
Texto del mensaje	Muestra una descripción del incidente registrado.
Permiso	La información sobre si la acción del usuario remoto se permite (concede) o no.
Categoría	El tipo de incidente registrado.
Tipo de fuente	El tipo de equipo en el que se produjo el incidente registrado, por ejemplo, servidor o dispositivo.
Nombre de la fuente	El nombre del equipo en el que se produjo el incidente registrado.
Usuario	El nombre de usuario del usuario remoto que causa el incidente registrado.
Ubicación del usuario	La dirección IP o el nombre de host del ordenador desde el que el usuario remoto causó el incidente registrado.

Registros desencadenados por reglas (pestaña)

Cada fila en un registro representa una entrada del registro. Una entrada de registro contiene una serie de campos de información:

Nombre	Descripción
Hora local	Con la marca de tiempo en la hora local del servidor de su sistema.
Texto del mensaje	Muestra una descripción del incidente registrado.
Categoría	El tipo de incidente registrado.
Tipo de fuente	El tipo de equipo en el que se produjo el incidente registrado, por ejemplo, servidor o dispositivo.
Nombre de la fuente	El nombre del equipo en el que se produjo el incidente registrado.
Tipo de evento	El tipo de evento representado por el incidente registrado.
Nombre de regla	El nombre de la regla que desencadena la entrada de registro.
Nombre de servicio	El nombre del servicio en el que ocurrió el incidente registrado.

Nodo de uso de metadatos

Metadatos y búsqueda de metadatos

Para gestionar y configurar dispositivos de metadatos, consulte Mostrar u ocultar categorías de búsqueda de metadatos y filtros de búsqueda en la página 307.

¿Qué son metadatos?

Los metadatos son datos sobre datos, por ejemplo, datos que describen la imagen del vídeo, el contenido o los objetos en la imagen, o la ubicación en la que se grabó la imagen.

Los metadatos pueden ser generados por:

- El propio dispositivo que proporciona los datos, por ejemplo, una cámara que proporciona vídeo
- Un sistema de terceros o la integración mediante un controlador de metadatos genérico

Búsqueda de metadatos

La búsqueda de metadatos es cualquier búsqueda de grabaciones de vídeo en XProtect Smart Client que utiliza categorías de búsqueda y filtros de búsqueda relacionados con los metadatos.

Las categorías de búsqueda de metadatos de Milestone predeterminadas son:

- Ubicación: Los usuarios pueden definir coordenadas geográficas y un radio de búsqueda a partir de dichas coordenadas.
- Gente: Los usuarios pueden buscar por sexo y estatura y edad aproximadas, así como seleccionar que se muestren resultados con rostros.
- Vehículos: Los usuarios pueden buscar por color, velocidad y tipo de vehículo, así como buscar una matrícula específica.

Requisitos de la búsqueda de metadatos

Para obtener resultados de búsqueda, necesita uno de los siguientes:

- Al menos un dispositivo de su sistema de videovigilancia puede realizar análisis de vídeo y está configurado correctamente
- Un servicio de procesamiento de vídeo en su sistema de videovigilancia que genera metadatos

En cualquier caso, los metadatos deben estar en el formato de metadatos requerido.

Si desea más información, consulte la documentación para la integración de la búsqueda de metadatos.

Nodo de control de acceso

Propiedades de control de acceso

Pestaña configuración general (control de acceso)

Nombre	Descripción
Habilitar	Los sistemas están habilitados por defecto, lo que significa que son visibles en XProtect Smart Client para los usuarios con permisos suficientes y que el sistema XProtect recibe eventos de control de acceso.

Nombre	Descripción
	Puede deshabilitar un sistema, por ejemplo durante el mantenimiento, para evitar la creación de alarmas innecesarias.
Nombre	El nombre de la integración del control de acceso tal y como aparece en la aplicación de gestión y en los clientes. Puede sobrescribir el nombre existente con uno nuevo.
Descripción	Proporciona una descripción de la integración del 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 la configuración	Muestra la fecha y hora de la última vez que se importó la configuración desde el sistema de control de acceso.
Actualizar configuración	Haga clic en el botón cuando necesite 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 de configuración del sistema de control de acceso. Revise la lista para garantizar que su sistema de control de acceso se refleja correctamente antes de aplicar la nueva configuración.
Es necesario que el operador inicie sesión	Habilita un inicio de sesión adicional para los usuarios del cliente, si el sistema de control de acceso admite permisos de usuario diferenciados. Si activa esta opción, el sistema de control de acceso no estará disponible en el cliente XProtect Mobile. Esta opción únicamente es visible si el complemento de integración admite permisos de usuario diferenciados.

Se importan los nombres y el contenido de los siguientes campos desde el complemento de integración. A continuación se muestran ejemplos de algunos campos típicos:

Nombre	Descripción
Dirección	Introduzca la dirección del servidor que aloja el sistema de control de acceso integrado.

Nombre	Descripción
Puerto	Especifique el número de puerto del servidor al que está conectado el sistema de control de acceso.
Nombre de usuario	Introduzca el nombre del usuario, según lo definido en el sistema de control de acceso, que debe ser administrador del sistema integrado en XProtect.
Contraseña	Especifique la contraseña del usuario.

Pestaña de puertas y cámaras asociadas (control de acceso)

Esta pestaña proporciona asignaciones entre los puntos de acceso de la puerta y las cámaras, los micrófonos o los altavoces. Asocia las cámaras como parte del asistente de integración, pero puede cambiar la configuración en cualquier momento. Las asignaciones a los micrófonos y altavoces están implícitas a través del micrófono o altavoz correspondiente de la cámara.

Nombre	Descripción
Puertas	Enumera los puntos de acceso de puerta disponibles definidos en el sistema de control de acceso, agrupados por puerta. Para una navegación más fácil hacia las puertas pertinentes, puede filtrar en las puertas de su sistema de control de acceso con el cuadro de lista desplegable en la parte superior. **Habilitado**: Las puertas con licencia están activadas por defecto. Puede deshabilitar una puerta para liberar una licencia. **Licencia**: Muestra si una puerta tiene licencia o si la licencia ha caducado. El campo está en blanco cuando la puerta está deshabilitada. **Borrar**: Haga clic en **Borrar** para eliminar una cámara de un punto de acceso. Si elimina todas las cámaras, la casilla de verificación de las cámaras asociadas se desactiva automáticamente.
Cámaras	Enumera las cámaras configuradas en el sistema XProtect. Seleccione una cámara de la lista y arrástrela al punto de acceso correspondiente para asociar el punto de acceso a la cámara.

Pestaña de eventos de control de acceso (control de acceso)

Las categorías de eventos le permiten agrupar eventos. La configuración de las categorías de eventos afecta al comportamiento del control de acceso en el sistema XProtect y le permite, por ejemplo, definir una alarma para que se active una única alarma en varios tipos de eventos.

Nombre	Descripción
Evento del control de acceso	Enumera los eventos de control de acceso importados desde el sistema de control de acceso. El plug-in de integración controla la activación y desactivación por defecto de los eventos. Puede habilitar o deshabilitar los eventos en cualquier momento después de la integración. Cuando se habilita un evento, se almacena en la base de datos de eventos XProtect y está, por ejemplo, disponible para el filtrado en el XProtect Smart Client.
Tipo de fuente	Muestra la unidad de control de acceso que puede activar el evento de control de acceso.
Categoría de evento	Asigne ninguna, una o más categorías de eventos a los eventos de control de acceso. El sistema asigna de forma automática las categorías de eventos correspondientes a los eventos durante la integración. Esto permite una configuración por defecto en el sistema XProtect. Puede cambiar la asignación en cualquier momento. Las categorías de eventos incorporadas son: • Acceso denegado • Acceso concedido • Petición de acceso • Alarma • Error • Advertencia Los eventos y las categorías de eventos definidos por el plug-in de integración también aparecen, pero también puede definir sus propias categorías de eventos, consulte **Categorías definidas por el usuario**. ⚠ Si cambia las categorías de eventos en XProtect Corporate, asegúrese de que las reglas de control de acceso existentes siguen funcionando.

Nombre	Descripción
Categorías definidas por el usuario	Le permite crear, modificar o eliminar categorías de eventos definidas por el usuario. Puede crear categorías de eventos cuando las categorías incorporadas no respondan a sus necesidades, por ejemplo, en relación con la definición de eventos activadores de acciones de control de acceso. Las categorías son globales para todos los sistemas de integración añadidos al sistema XProtect. Permiten configurar la gestión entre sistemas, por ejemplo, en las definiciones de las alarmas. Si elimina una categoría de eventos definida por el usuario, recibirá una advertencia si es utilizada por alguna integración. Si la elimina de 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 determinado evento.

Nombre	Descripción
Nombre	Introduzca un nombre para la notificación de solicitud de acceso.
Añadir notificación de petición de acceso	Haga clic para añadir y definir las notificaciones de solicitud de acceso. Para eliminar una notificación, haga clic en la **X** en el lado derecho.  Si un usuario de XProtect Smart Client inicia sesión en un sitio principal en una jerarquía Milestone Federated Architecture, las notificaciones de solicitud de acceso de los sitios secundarios también aparecen en XProtect Smart Client.
Detalles de notificación de petición de acceso	Especifica qué cámaras, micrófonos o altavoces aparecen en las notificaciones de solicitud de acceso cuando se produce un determinado evento. También especifica el sonido para alertar al usuario cuando aparezca la notificación.

Nombre	Descripción
Añadir comando	Selecciona los comandos que deben estar disponibles como botones en los diálogos de notificación de solicitud de acceso en el XProtect Smart Client. Comandos de solicitud de acceso relacionados: • Habilita todos los comandos relacionados con las operaciones de solicitud de acceso disponibles en la unidad de origen. Por ejemplo **Abrir puerta** Todos los comandos relacionados: • Habilita todos los comandos en la unidad de origen Comando de control de acceso: • Habilita un comando de control de acceso seleccionado Comando de sistema: • Habilita un comando predefinido en el sistema XProtect Para eliminar un comando, haga clic en la **X** en el lado derecho.

Pestaña de poseedores de tarjetas (control de acceso)

Utilice la pestaña **Poseedores de tarjetas** para revisar la información sobre los poseedores de tarjetas en el sistema de control de acceso.

Nombre	Descripción
Buscar propietario de tarjeta	Introduzca los caracteres de un nombre de poseedor de tarjeta y aparecerá en la lista, si existe.
Nombre	Enumera los nombres de los poseedores de tarjetas recuperados del sistema de control de acceso.
Tipo	Enumera el tipo de poseedor de tarjeta, por ejemplo: • Empleado • Guardia • Invitado

Si su sistema de control de acceso admite la adición/eliminación de imágenes en el sistema XProtect, puede añadir imágenes a los poseedores de tarjetas. Esto es útil si su sistema de control de acceso no incluye imágenes de los poseedores de tarjetas.

Nombre	Descripción
Seleccionar imagen	Especifica la ruta de acceso a un archivo con una imagen del poseedor de la tarjeta. Este botón no es visible si el sistema de control de acceso gestiona las imágenes. Los formatos de archivo permitidos son .bmp, .png, y .jpg. Las imágenes se redimensionan para maximizar la vista. Milestone recomienda utilizar un cuadro cuadrático.
Eliminar imagen	Haga clic para eliminar la imagen. Si el sistema de control de acceso tenía una imagen, esta imagen se muestra después de la eliminación.

Nodo de incidentes

Propiedades del incidente (nodo Incidentes)

La siguiente información describe ajustes relacionados con XProtect Incident Manager.

Define todas las propiedades del incidente para sus operadores de XProtect Smart Client en estas pestañas:

- Tipos
- Estados
- Categorías
- Categoría 1-5

Todas las propiedades de incidentes tienen los siguientes ajustes:

Nombre	Descripción
Nombre	Los nombres de propiedades de incidentes no tienen por qué ser únicos, pero utilizar nombres de propiedades de incidentes únicos y descriptivos es una ventaja en muchas situaciones.

Nombre	Descripción
Descripción	Una explicación más detallada de la propiedad del incidente definida. Por ejemplo, si ha creado una categoría llamada *Ubicación*, su descripción podría ser *¿Dónde ocurrió el incidente?*

Nodo de transacción

Fuentes de transacciones (nodo Transacción)

La tabla siguiente describe las propiedades para fuentes de transacciones.

Si desea más información acerca de añadir una cuenta, consulte Añadir fuente de transacción (asistente).

Fuentes de transacción (propiedades)

Nombre	Descripción
Habilitar	Si desea deshabilitar la fuente de transacciones, desmarque esta casilla. El flujo de datos de la transacción se detiene, pero los datos ya importados permanecen en el servidor de eventos. Puede seguir viendo las transacciones de una fuente de transacción deshabilitada en XProtect Smart Client durante su período de retención. Incluso una fuente de transacciones desactivada requiere una licencia de fuente de transacción.
Nombre	Si desea cambiar el nombre, introduzca un nuevo nombre aquí.
Conector	No puede cambiar el conector que seleccionó cuando creó la fuente de la transacción. Para seleccionar un conector diferente, debe crear una nueva fuente de transacciones y, durante el asistente, seleccionar el conector que desee.
Definición de la transacción	Puede seleccionar una definición de transacción diferente que defina cómo transformar los datos de transacción recibidos en transacciones y líneas de transacción. Esto incluye definir: • Cuando comienza y termina una transacción

Nombre	Descripción
	• Cómo se muestran las transacciones en XProtect Smart Client
Periodo de retención	Especifica, en días, durante cuánto tiempo se mantienen los datos de las transacciones en el servidor de eventos. El periodo de retención por defecto es de 30 días. Cuando el periodo de retención concluye, los datos se eliminan automáticamente. Esto es para evitar la situación en la que se supera la capacidad de almacenamiento de la base de datos. El valor mínimo es de 1 día, mientras que el valor máximo es de 1000 días.
Conector de cliente TCP	Si ha seleccionado el **conector de cliente TCP**, especifique esta configuración: • **Nombre de host**: introduzca el nombre de host del servidor TCP asociado al origen de la transacción • **Puerto**: introduzca el nombre del puerto del servidor TCP asociado al origen de la transacciónsource
Conector de puerto serial	Si ha seleccionado el **Conector de puerto serie**, especifique estos ajustes y asegúrese de que coinciden con los del origen de la transacción: • **Puerto de serie**: seleccione el puerto COM • **Velocidad de baudio**: especifique el número de bits transmitidos por segundo • **Paridad**: especifique el método de detección de errores en las transmisiones. Por defecto, se selecciona **Ninguno** • **Bits de datos**: especifique el número de bits utilizados para representar un carácter de datos • **Detener bits**: especifique el número de bits para indicar cuándo se ha transmitido un byte. La mayoría de los dispositivos necesitan 1 bit • **Handshake**: especifica el método de negociación que determina el protocolo de comunicación entre el origen de la transacción y el servidor de eventos

Definiciones de transacciones (nodo Transacción)

La tabla siguiente describe las propiedades para definiciones que se deben a usar para las fuentes de transacciones.

Si desea más información sobre cómo crear y añadir definiciones de transacciones, consulte Crear y añadir definiciones de transacciones.

Definiciones de transacciones (propiedades)

Nombre	Descripción
Nombre	Introduzca un nombre.
Codificación	Seleccione el juego de caracteres utilizado por la fuente de la transacción, por ejemplo la caja registradora. Esto ayuda a XProtect Transact a convertir los datos de la transacción en un texto comprensible con el que se puede trabajar al configurar la definición. Si selecciona la codificación incorrecta, los datos pueden aparecer como un texto sin sentido.
Iniciar a recopilar datos	Recopile datos de transacciones de la fuente de transacciones conectada. Puede utilizar los datos para configurar una definición de transacción. Espere a que se complete al menos una, pero preferiblemente más, transacciones.
Dejar de recopilar datos	Cuando haya recopilado suficientes datos para configurar la definición, haga clic en este botón.
Cargar desde un archivo	Si desea importar datos de un archivo ya existente, haga clic en este botón. Normalmente se trata de un archivo que ha creado previamente en el formato de archivo .capture. Pueden ser otros formatos de archivo. Lo importante aquí es que la codificación del archivo de importación coincida con la codificación seleccionada para la definición actual.
Guardar en archivo	Si desea guardar los datos brutos recogidos en un archivo, haga clic en este botón. Puede reutilizarlo más tarde.
Tipo de coincidencia	Seleccione el tipo de coincidencia que se utilizará para buscar el patrón de inicio y el patrón de detención en los datos brutos recogidos: • Usar coincidencia exacta: La búsqueda identifica las cadenas que contienen lo que ha introducido en los campos **Patrón de inicio** y **Patrón de detención**

Nombre	Descripción
	• Usar comodines: La búsqueda identifica las cadenas que contienen lo que ha introducido en los campos **Patrón de inicio** y **Patrón de detención** en combinación con un símbolo de comodín (*, #, ?) * coincide con cualquier número de caracteres. Por ejemplo, si ha introducido "Iniciar tra*ción", la búsqueda identifica las cadenas que contienen "Iniciar transacción". # coincide exactamente con 1 dígito. Por ejemplo, si ha introducido "#sandía", la búsqueda identifica las cadenas que contienen, por ejemplo, "1 sandía". ? coincide exactamente con 1 carácter. Por ejemplo, puede utilizar la expresión de búsqueda "Iniciar trans?cción" para identificar las cadenas que contengan "Iniciar transacción" • Usar expresión normal: Use este tipo de coincidencia para identificar cadenas que contengan métodos de notación o convenciones específicas, por ejemplo un formato de fecha o un número de tarjeta de crédito. Para obtener más información, consulte el sitio web de Microsoft (https://docs.microsoft.com/dotnet/standard/base-types/regular-expression-language-quick-reference/)
Datos base	Las cadenas de datos de las transacciones de la fuente de transacciones conectada se muestran en esta sección.
Patrón de inicio	Especifica un patrón de inicio para indicar dónde comienza una transacción. Las líneas horizontales están insertadas en el campo de **Vista previa** para visualizar dónde empieza y termina la transacción, y ayudarán a mantener separadas las transacciones individuales.
Patrón de detención	Especificar un patrón de detención para indicar dónde termina una transacción. Un patrón de detención no es obligatorio, pero es útil si los datos recibidos contienen información irrelevante, como información sobre horarios de apertura u ofertas especiales, entre las transacciones reales. Si no se especifica un patrón de detención, el final del recibo se define en términos de dónde comienza el siguiente recibo. El inicio se determina por lo que se introduce en el campo **Patrón de inicio**.
Añadir filtro	Utilice el botón **Añadir filtros** para señalar los caracteres que desea omitir en XProtect Smart Client o sustituir por otros o por un salto de línea.

Nombre	Descripción
	La sustitución de caracteres es útil cuando la cadena de origen de la transacción contiene caracteres de control para fines no relacionados con la impresión. Es necesario añadir saltos de línea para que los recibos en XProtect Smart Client se parezcan a los originales.
Texto de filtro	Muestra los caracteres actualmente seleccionados en la sección de **Datos base**. Si conoce los caracteres que desea omitir o sustituir, pero no aparecen en la cadena de datos brutos recogida, puede introducir los caracteres manualmente en el campo **Carácter**. Si el carácter es de control, deberá introducir su valor hexadecimal en bytes. Utilice este formato para el valor del byte: {XX} y {XX, XX,...} si un carácter consta de más bytes.
Acción	Para cada filtro que añada, debe especificar cómo se manejan los caracteres que ha seleccionado: • Omitir: se filtran los caracteres seleccionados • Sustituir: los caracteres que seleccione serán sustituidos por los caracteres que especifique • Añadir salto de línea: los caracteres que seleccione serán sustituidos por un salto de línea
Sustitución	Introduzca el texto para sustituir los caracteres seleccionados. Solo es relevante si ha seleccionado la acción **Sustituir**.
Elimine los caracteres de control que no están definidos como texto de filtro	Elimine los caracteres no imprimibles que no se hayan eliminado ya después de añadir los filtros. En el panel de **Datos base** y en la sección de **Vista previa**, vea cómo cambian las cadenas de datos de las transacciones cuando habilita o deshabilita esta configuración.
Previsualizar	Utilice la sección **Vista previa** para verificar que ha identificado y filtrado los caracteres no deseados. La salida que ve aquí se asemeja a lo que es el recibo en la vida real en XProtect Smart Client.

Nodo de alarmas

Definiciones de alarmas (nodo Alarmas)

Cuando el sistema registra un evento en su sistema, puede configurar el sistema para generar una alarman en XProtect Smart Client. Debe definir alarmas antes de poder usarlas, y las alarmas se definen en función de los eventos registrados en los servidores del sistema. También puede utilizar eventos definidos por el usuario para desencadenar alarmas y utilizar el mismo evento para desencadenar varias alarmas distintas.

Ajustes de definición de alarmas:

Nombre	Descripción
Habilitar	De forma predeterminada, la definición de la alarma se habilita. Para deshabilitarlo, desactive la casilla de verificación.
Nombre	Los nombres de alarmas no tienen por qué ser únicos, pero utilizar nombres de alarma únicos y descriptivos resulta ventajoso en muchas situaciones.
Instrucciones	Introduzca un texto descriptivo sobre la alarma y cómo resolver el problema que causó la alarma. El texto aparece en XProtect Smart Client cuando el usuario maneja la alarma.
Evento activador	Seleccione el mensaje del evento que usar cuando la alarma se desencadene. Elija de los dos menús desplegables: • El primer menú desplegable: Seleccionar el tipo de evento, por ejemplo, evento de análisis o eventos del sistemas • El segundo desplegable: Seleccione el mensaje del evento concreto que usar. Los mensajes disponibles vienen determinados por el tipo de evento que seleccione en el primer menú desplegable
Fuentes	Especifique las fuentes de las que se originan los eventos. Aparte de cámaras u otros dispositivos, las fuentes también pueden ser fuentes definidas de plug-in, por ejemplo, VCA y MIP. Las opciones dependen del tipo de evento que haya seleccionado.

Desencadenante de alarmas:

Nombre	Descripción
Perfil temporal	Seleccione el botón de opción **Perfil temporal** para especificar el intervalo de tiempo durante el cual la definición de la alarma está activa. Solo el perfil temporal que ha definido en el nodo **Reglas y Eventos** se muestra en la lista. Si no se ha definido ninguno, solo está disponible la opción **Siempre**.
Basado en eventos	Si quiere que la alarma se base en un evento, seleccione este botón de opción. Una vez seleccionado, especifique el evento de inicio y parada. Puede seleccionar eventos de hardware definidos en cámaras, servidores de vídeo y entrada. Consulte también Descripción general de eventos. También se pueden usar definiciones de eventos globales/manuales. Consulte también Eventos definidos por el usuario (explicación).

Acción del opreador requerida:

Nombre	Descripción
Límite de tiempo	Seleccione un límite de tiempo para cuando se requiere la acción del operador. El valor predeterminado es 1 minuto. El límite de tiempo no se activa antes de haber adjuntado un evento en el menú desplegable **Eventos desencadenados**.
Eventos activados	Seleccione qué evento desencadenar cuando se pase el límite de tiempo.

Planos:

Nombre	Descripción
Vista de Gestor de alarmas	Asignar un plano inteligente o un plano a la alarma cuando la alarma aparezca en XProtect Smart Client > **Gestor de alarmas**. El plano inteligente muestra las alarmas si son activadas por un dispositivo y si el dispositivo se añade al plano inteligente.

Otro:

Nombre	Descripción
Cámaras relacionadas	Seleccione un máximo de 15 cámaras para incluir en la definición de alarma, incluso si esas cámaras no desencadenan ellas mismas la alarma. Este artículo puede ser relevante, por ejemplo, si ha seleccionado un mensaje de evento externo (como la apertura de una puerta) como fuente de su alarma. Al definir una o más cámaras cerca de la puerta, puede adjuntar las grabaciones de las cámaras del incidente a la alarma.
Propietario de la alarma inicial	Seleccione un usuario predeterminado responsable de la alarma.
Prioridad de la alarma inicial	Seleccione una prioridad para la alarma. Utilice estas prioridades en XProtect Smart Client para determinar la importancia de una alarma.
Categoría de alarma	Seleccione una categoría de alarma para la alarma, por ejemplo **Falsa alarma** o **Necesita investigación**.
Eventos desencadenados por alarma	Defina un evento que la alarma pueda desencadenar en XProtect Smart Client.
Alarma de cierre automático	Si quiere que un evento particular detenga automáticamente la alarma, seleccione esta casilla de verificación. No todos los eventos pueden desencadenar alarmas. Desactive la casilla de verificación para deshabilitar la nueva alarma desde el principio.
Alarma asignable a administradores	Seleccione la casilla de verificación para incluir usuarios con un rol de administrador en la lista **Asignado a**. La lista **Asignado a** está en los detalles de la alarma en la pestaña **Gestor de alarmas** en XProtect Smart Client. Desactive la casilla de verificación para filtrar por usuarios con un rol de administrador de la lista **Asignado a** para reducir la lista.

Ajustes de datos de alarmas (nodo Alarmas)

Cuando configure ajustes de datos de alarmas, especifique lo siguiente:

Pestaña Niveles de datos de alarmas

Prioridades

Nombre	Descripción
Nivel	Añadir periodicidades nuevas con números de nivel de su elección o usar/editar los niveles de prioridad predeterminados (números 1, 2 o 3). Estos niveles de prioridad se usan para configurar el ajuste **Prioridad de la alarma inicial**.
Nombre	Introducir un nombre para la entidad. Puede crear tantos como quiera.
Sonido	Seleccione el sonido que se debe asociar a la alarma. Utilice uno de los sonidos predeterminados o añada más en **Ajustes de sonido**.
Repetir sonido	Decida si el sonido debe reproducirse solo una vez o repetidamente hasta que el operador hace clic en la alarma en la lista de alarmas en XProtect Smart Client.
Habilitar notificaciones de escritorio	Para cada prioridad de alarma, puede habilitar o deshabilitar las notificaciones de escritorio. Si está utilizando un XProtect VMS que admite Smart Client perfiles, también debe habilitar notificaciones en los perfiles de Smart Client requeridos. Consulte Pestaña Gestor de alarmas (perfiles de Smart Client) en la página 492.

Estados

Nombre	Descripción
Nivel	Además de los niveles de estado prefeterminados (números **1**, **4**, **9** y **11**, que no se pueden editar ni reutilizar), añada nuevos estados con los números de nivel que elija. Estos niveles de estado solo son visibles en la *Lista de alarmas* de XProtect Smart Client.

Categorías

Nombre	Descripción
Nivel	Añadir categorías nuevas con números de nivel de su elección. Estos niveles de categoría se utilizan para configurar el ajuste **Categoría de alarma inicial**.
Nombre	Introducir un nombre para la entidad. Puede crear tantos como quiera.

Pestaña Configuración de lista de alarmas

Nombre	Descripción
Columnas disponibles	Utilice > para seleccionar qué columnas deben estar disponibles en la *Lista de alarmas* de XProtect Smart Client. Utilice < para borrar la selección. Cuando haya terminado, **Columnas seleccionadas** debe contener los elementos que se deben incluir.

Pestaña Motivos para el cierre

Nombre	Descripción
Habilitar	Seleccione para habilitar que todas las alarmas deben asignarse a un motivo de cierre antes de que se puedan cerrar.
Motivo	Añadir motivos para cerrar entre los que el usuario puede elegir al cerrar alarmas. Ejemplos podrían ser *Intruso resuelto* o *Falsa alarma*. Puede crear tantos como quiera.

Ajustes de sonido (nodo Alarmas)

Cuando se configuran los ajustes de sonido, especifique lo siguiente:

Nombre	Descripción
Sonidos	Seleccione el sonido que se debe asociar a la alarma. La lista de sonidos contiene un número de sonidos de Windows predeterminados. También puede añadir nuevos sonidos (.wav o .mp3).
Añadir	Añadir Sonidos. Busque el archivo de sonido y cargue uno o varios archivos .wav o .mp3.
Borrar	Quite un sonido seleccionado desde la lista de sonidos añadidos manualmente. Los sonidos predeterminados no se pueden eliminar.
Prueba	Pruebe el sonido. En la lista, seleccione el sonido. El sonido se reproduce una vez.

Jerarquía de sitios federados

Propiedades de sitio federado

Esta sección describe la pestaña **General** y la pestaña **Sitio principal**.

Pestaña general

Puede cambiar parte de la información relacionada con el sitio en el que ha iniciado la sesión.

Nombre	Descripción
Nombre	Introduzca el nombre del sitio.
Descripción	Introduzca una descripción del sitio.
URL	Utilice la lista para añadir y eliminar URL(s) para este sitio e indicar si son externas o no. Las direcciones externas son accesibles desde fuera de la red local.
Versión	El número de versión del servidor de gestión del sitio.
Cuenta de servicio	La cuenta de servicio bajo la que se ejecuta el servidor de gestión.
Hora para la	Hora y fecha de la última sincronización de la jerarquía.

Nombre	Descripción
última sincronización	
Estado para la última sincronización	El estado de la última sincronización de la jerarquía. Puede ser **Exitoso** o **Fallido**.

Pestaña del sitio principal

Esta pestaña muestra información sobre el sitio principal del sitio en el que está iniciado sesión. La pestaña no es visible si su sitio no tiene un sitio principal.

Nombre	Descripción
Nombre	Muestra el nombre del sitio principal.
Descripción	Muestra una descripción del sitio principal (opcional).
URL	Enumera la(s) URL(s) del sitio principal e indica si son externas o no. Las direcciones externas son accesibles desde fuera de la red local.
Versión	El número de versión del servidor de gestión del sitio.
Cuenta de servicio	La cuenta de servicio bajo la que se ejecuta el servidor de gestión.
Hora para 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 **Exitoso** o **Fallido**.

helpfeedback@milestone.dk

Acerca de Milestone

Milestone Systems figura entre los proveedores más destacados de software de gestión de vídeo de plataforma abierta, tecnología que ayuda a determinar cómo garantizar la seguridad, proteger 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, gracias a soluciones fiables y escalables de eficacia probada en más de 150 000 instalaciones de todo el mundo. Milestone Systems se fundó en 1998 y es una empresa independiente dentro del Canon Group. Para obtener más información, visite https://www.milestonesys.com/.