



Guía del Usuario del Dispositivo Streamvault™

Haga clic [aquí](#) para obtener la versión más reciente de este documento.

El documento se actualizó por última vez: 5 de junio de 2025

Avisos legales

©2025 Genetec Inc. Todos los derechos reservados.

Genetec Inc. distribuye este documento con software que incluye un convenio de licencia de usuario final, se suministra bajo licencia y solo puede usarse de acuerdo con los términos del convenio de la licencia. El contenido de este documento está protegido por las leyes de copyright.

El contenido de esta guía es solo para uso informativo y está sujeto a cambios sin previo aviso. Genetec Inc. no asume ninguna responsabilidad u obligación legal por cualquier error o inexactitud que pueda aparecer en el contenido informativo de esta guía.

Esta publicación no puede ser copiada, modificada o reproducida de manera alguna ni para propósito alguno, ni se puede crear ninguna obra derivada de la misma sin previo consentimiento escrito de Genetec Inc.

Genetec Inc. se reserva al derecho a revisar y mejorar sus productos según estime conveniente. Este documento describe el estado de un producto en el momento de la última revisión del documento, y puede que no refleje el producto en todo momento en el futuro.

En ningún caso Genetec Inc. será responsable ante ninguna persona o entidad con respecto a cualquier pérdida o daño que sea incidental o resultante de las instrucciones que se encuentran en este documento o los productos de software y hardware descritos en este documento.

Genetec™, AutoVu™, AutoVu MLC™, Citywise™, Cloud Link Roadrunner™, Community Connect™, Curb Sense™, Federation™, Flexreader™, Genetec Airport Sense™, Genetec Citigraf™, Genetec Clearance™, Genetec ClearID™, Genetec Cloudlink™, Genetec Mission Control™, Genetec Motoscan™, Genetec Patroller™, Genetec Retail Sense™, Genetec Traffic Sense™, KiwiVision™, KiwiSecurity™, Omnicast™, Privacy Protector™, Sipelia™, Stratocast™, Streamvault™, Streamvault Edge™, Synergis™, Valcri™, sus respectivos logotipos y el logotipo de la banda de Möbius son marcas comerciales de Genetec Inc. y pueden estar registradas o pendientes de registro en varias jurisdicciones.

Otras marcas comerciales utilizadas en este documento pueden ser marcas comerciales de los fabricantes o proveedores de los productos respectivos.

Patente pendiente. Genetec™ Security Center, Omnicast™, AutoVu™, Stratocast™, Genetec Citigraf™, Genetec Clearance™ y otros productos de Genetec™ son objeto de solicitudes de patente pendientes y pueden ser objeto de patentes emitidas en los Estados Unidos y en otras jurisdicciones del mundo.

Todas las especificaciones están sujetas a cambios sin previo aviso.

Información del Documento

Título del documento: Guía del Usuario del Dispositivo Streamvault™

Número de documento original: EN.803.003

Número del Documento: ES.803.003

Fecha de actualización del documento: 5 de junio de 2025

Puede enviar sus comentarios, correcciones y sugerencias sobre esta guía a documentation@genetec.com.

Acerca de esta guía

Esta guía explica cómo instalar y configurar su dispositivo Streamvault para que funcione con el control de acceso y la videovigilancia de Security Center utilizando la versión actual del SV Control Panel. Esta guía complementa la Guía del administrador de Security Center y la Guía de configuración del dispositivo Synergis™.

Esta guía está escrita para el integrador que realiza la configuración inicial del dispositivo SV. Se presume que usted está familiarizado con la terminología y los conceptos utilizados en Security Center.

Notas y avisos

Las siguientes notas y avisos pueden aparecer en esta guía:

- **Sugerencia:** Sugiere cómo aplicar la información en un tema o paso.
- **Nota:** Explica un caso especial o amplía un punto importante.
- **Importante:** Señala información crítica sobre un tema o paso.
- **Precaución:** Indica que una acción o paso puede provocar la pérdida de datos, problemas de seguridad o problemas de rendimiento.
- **Advertencia:** Indica que una acción o paso puede provocar daños físicos o dañar el hardware.

IMPORTANTE: El contenido de esta guía que hace referencia a la información que se encuentra en sitios web de terceros era precisa en el momento de la publicación; sin embargo, esta información está sujeta a cambios sin previo aviso de Genetec Inc.

Contenido

Preface

Avisos legales.	ii
Acerca de esta guía.	iii

Capítulo 1: Introducción a su dispositivo Streamvault

Primeros pasos con su dispositivo Streamvault.	2
Puertos predeterminados utilizados por Streamvault.	4
Acerca de la actualización del software de SV en el SV Control Panel.	7
Conectar los componentes del dispositivo Streamvault.	8
Tarjetas codificadoras analógicas de Genetec.	8
Deshabilitar las entradas de cámara en tarjetas codificadoras en el dispositivo Streamvault.	9
Entradas y salidas de alarma de un Streamvault aparato.	10
Acerca de las cuentas de usuario de Streamvault.	12
Información de inicio de sesión para las cuentas de usuario predeterminadas en un dispositivo Streamvault.	12
Iniciar sesión en un Streamvault aparato.	14
Acerca del servicio Streamvault.	15
Acerca del endurecimiento de Streamvault.	16
Dispositivos con capacidades de administración de endurecimiento.	16

Capítulo 2: Introducción a SV Control Panel

Acerca del panel de control de SV.	19
Configuración de su dispositivo en SV Control Panel.	19
Activación de su licencia de Security Center en un dispositivo.	22
Activar una licencia de manera manual desde el Server Admin.	24
Activar System Availability Monitor.	26
Habilitación de las características de control de acceso y video de Security Center.	27
Acerca de la Herramienta de Inscripción de la Unidad.	30
Abrir la Herramienta de inscripción de la Unidad.	30
Configurar los ajustes de inscripción de la unidad.	30
Agregar unidades.	31
Borrar unidades agregadas.	31
Ignorando unidades.	32
Eliminar unidades de la lista de unidades ignoradas.	32
Configurar los ajustes predeterminados de la cámara.	33
Crear horarios de grabación personalizados.	35
Acerca de la copia de respaldo y la restauración.	36
Crear una copia de respaldo de la base de datos de su Directory.	37
Restaurar la base de datos de su Directory.	38
Elegir el método para crear funciones y particiones del Archiver.	39
Añadir funciones de Archiver en SV Control Panel.	39
Agregar particiones y funciones del Archiver de manera manual.	41
Cifrado de la unidad del SO.	44
Creación de una clave de recuperación.	45
Recopilación de registros de soporte.	48

Capítulo 3: Primeros pasos con el plugin Streamvault Maintenance

Acerca de Streamvault Maintenance enchufar.	51
Descargando e instalando el complemento.	52
Privilegios de Genetec Streamvault.	53
Crear la función de plugin.	55
Configuración de una entidad de monitorización de hardware de Streamvault.	56
Configurar una entidad de administrador de Streamvault.	60
Acerca de la pestaña de Administración.	63
Revisar la salud del dispositivo Streamvault.	64
Columnas del panel de informes para la tarea de hardware de Streamvault.	65
Creación de eventos a toma de acción para eventos de estado de Streamvault.	66

Capítulo 4: Referencia de SV Control Panel

Página de inicio de SV Control Panel.	69
Página de configuración del Panel de Control SV.	71
Página de seguridad del SV Control Panel.	74
Acerca de la página de SV Control Panel.	78

Capítulo 5: Recursos adicionales

Garantía de producto de su dispositivo Streamvault.	81
Configuración de la contraseña de BIOS.	82
Cambio de la contraseña predeterminada de iDRAC.	85
Cómo agregar un nuevo usuario de iDRAC con privilegios de administrador.	86
Cómo deshabilitar el usuario raíz de iDRAC.	87
Restablecer la imagen de un dispositivo Streamvault.	88
Encontrar la ID del sistema y la versión de la imagen de un dispositivo Streamvault.	89
Permitir compartir archivos en un dispositivo Streamvault.	90
Permitir conexiones a Escritorio Remoto con un dispositivo Streamvault.	91

Capítulo 6: Solución de problemas

Realizar un restablecimiento de fábrica en un dispositivo todo en uno Streamvault.	93
Crear una memoria USB con restablecimiento de fábrica para un dispositivo Streamvault Todo en Uno.	93
Restablecer la imagen del software en un dispositivo todo en uno.	95
Realizar un restablecimiento de fábrica en un Streamvault estación de trabajo o dispositivo servidor.	104
Crear una memoria USB de restablecimiento de fábrica para una estación de trabajo o dispositivo de servidor Streamvault.	104
Restablecer la imagen del software en una Streamvault estación de trabajo o un dispositivo servidor.	106
Los controladores Mercury EP permanecen fuera de línea cuando TLS 1.1 está desactivado.	109
Habilitación de la seguridad de la capa de transporte (TLS).	110
El Escritorio remoto no se puede conectar a un dispositivo Streamvault.	113
Cómo eliminar restricciones de cuentas de usuarios que no son administradores.	117
Las cuentas locales no pueden acceder al Escritorio remoto, al servicio de uso compartido de archivos y a la administración remota.	118
Habilitación de servicios relacionados con Tarjetas Inteligentes.	119
Habilitación de la compatibilidad con controladores Mercury EP y LP firmware 1.x.x.	120
Habilitación del soporte para la integración de Synergis IX.	122
Modificación de GPO locales para cuentas de usuarios no administradores.	123
Cómo desactivar el firewall de Windows.	126

Capítulo 7: Apoyo técnico

Comunicación con el Centro de Asistencia Técnica de Genetec. 129

 Contactar con GTAC por teléfono. 129

 Contactando con el GTAC a través de GTAP. 130

 Contactando con el GTAC a través del chat en vivo. 130

Soporte de software. 132

Soporte de hardware. 133

Especificaciones para Streamvault. 134

Términos y condiciones del soporte de Streamvault. 135

Glosario 136

Dónde encontrar información del producto 138

Introducción a su dispositivo Streamvault

Esta sección incluye los temas siguientes:

- ["Primeros pasos con su dispositivo Streamvault"](#) en la página 2
- ["Puertos predeterminados utilizados por Streamvault"](#) en la página 4
- ["Acerca de la actualización del software de SV en el SV Control Panel"](#) en la página 7
- ["Conectar los componentes del dispositivo Streamvault"](#) en la página 8
- ["Acerca de las cuentas de usuario de Streamvault"](#) en la página 12
- ["Iniciar sesión en un Streamvault aparato"](#) en la página 14
- ["Acerca del servicio Streamvault"](#) en la página 15
- ["Acerca del endurecimiento de Streamvault"](#) en la página 16

Primeros pasos con su dispositivo Streamvault

Puede implementar su dispositivo Streamvault™ en Security Center al completar una secuencia de pasos.

Descripción general de la implementación

Paso	Tarea	Dónde encontrar más información
Comprender los requisitos previos y los problemas clave antes de implementar		
1	Abra los puertos de red necesarios para conectar los sistemas centrales en Security Center y los módulos de Streamvault. Conecte los periféricos, como el monitor, el teclado, la tarjeta codificadora analógica y los dispositivos a las entradas y salidas. Conecte el dispositivo a su red.	<ul style="list-style-type: none"> • Puertos predeterminados utilizados por Streamvault en la página 4. • Conectar los componentes del dispositivo Streamvault en la página 8. • Tarjetas codificadoras analógicas de Genetec en la página 8. • Deshabilitar las entradas de cámara en tarjetas codificadoras en el dispositivo Streamvault en la página 9. • Entradas y salidas de alarma de un Streamvault aparato en la página 10.
2	Antes de implementar su dispositivo, conozca el contenido de la versión de su imagen.	<ul style="list-style-type: none"> • Contenido de cada lanzamiento de imagen de Streamvault.
3	Inicie sesión en Windows como Administrador con la contraseña que está impresa en su dispositivo y, luego, cambie la contraseña.	<ul style="list-style-type: none"> • Iniciar sesión en un Streamvault aparato en la página 14.
4	Configure la contraseña de BIOS en su dispositivo.	<ul style="list-style-type: none"> • Configuración de la contraseña de BIOS en la página 82.
5	Si su dispositivo admite iDRAC, cambie la contraseña de iDRAC predeterminada de inmediato. Para mayor seguridad, se recomienda crear una cuenta de usuario alternativa con privilegios administrativos y deshabilitar la cuenta de usuario raíz.	<ul style="list-style-type: none"> • Cambio de la contraseña predeterminada de iDRAC en la página 85. • Cómo agregar un nuevo usuario de iDRAC con privilegios de administrador en la página 86. • Cómo deshabilitar el usuario raíz de iDRAC en la página 87.
Complete los asistentes de configuración		
6	Complete el asistente de <i>configuración de Streamvault Control Panel</i> . NOTA: El escritorio remoto está deshabilitado de manera predeterminada. Para habilitar el escritorio remoto, active la configuración de Servicio de Escritorio Remoto en la página de <i>Seguridad</i> de SV Control Panel.	<ul style="list-style-type: none"> • Configuración de su dispositivo en SV Control Panel en la página 19. • Permitir conexiones a Escritorio Remoto con un dispositivo Streamvault en la página 91.

Paso	Tarea	Dónde encontrar más información
7	<p>Active su licencia de Security Center.</p> <ul style="list-style-type: none"> Si el dispositivo está conectado a internet, active su licencia mediante el asistente de <i>Activación del Panel de Control de Streamvault</i>. Si el dispositivo no está conectado a internet, active su licencia de forma manual desde Server Admin. 	<ul style="list-style-type: none"> Activación de su licencia de Security Center en un dispositivo en la página 22. Activar una licencia de manera manual desde el Server Admin en la página 24.
8	Active System Availability Monitor.	<ul style="list-style-type: none"> Activar System Availability Monitor en la página 26.
9	Configure Genetec™ Update Service para poder obtener la última versión de Security Center y SV Control Panel. Si hay actualizaciones, instálelas.	<ul style="list-style-type: none"> Configurar Genetec Update Service.
10	Si SV Control Panel indica que hay más actualizaciones disponibles, instálelas ahora.	<ul style="list-style-type: none"> Acerca de la actualización del software de SV en el SV Control Panel en la página 7.
11	Cifre la unidad del SO en su dispositivo con BitLocker y cree una clave de recuperación.	<ul style="list-style-type: none"> Cifrado de la unidad del SO en la página 44.
12	Para un dispositivo Archiver, cree la cantidad de funciones del Archiver que necesita para admitir la cantidad de cámaras y el ancho de banda total de la red planificado para su implementación.	<ul style="list-style-type: none"> Para las series SV-1000E, SV-2000E, SV-4000E: Añadir funciones de Archiver en SV Control Panel en la página 39. Para SV-7000EX y para dispositivos Todo en uno: Agregar particiones y funciones del Archiver de manera manual en la página 41.
13	Inicie sesión en Config Tool y configure sus características de video y control de acceso de Security Center.	<ul style="list-style-type: none"> Habilitación de las características de control de acceso y video de Security Center en la página 27. Configurar los ajustes de inscripción de la unidad en la página 30.
14	Realice una copia de respaldo de la configuración de Security Center.	<ul style="list-style-type: none"> Crear una copia de respaldo de la base de datos de su Directory en la página 37.

Puertos predeterminados utilizados por Streamvault

Los puertos de red requeridos deben abrirse para permitir que los siguientes componentes de Streamvault™ funcionen de manera correcta.

Puertos requeridos del complemento de mantenimiento Streamvault

El siguiente puerto debe abrirse en un firewall externo para el tráfico entrante, de modo que el plugin de mantenimiento de Streamvault™ pueda comunicarse con el hardware de Streamvault. Este requisito solo se aplica si se cumplen las tres condiciones siguientes:

- La conexión interna de paso a través del sistema operativo a iDRAC está deshabilitada
- El iDRAC utiliza un puerto LAN exclusivo
- Hay un firewall entre la red de iDRAC y la red anfitriona

En cualquier otra situación, se puede ignorar este requisito.

Módulo	Puerto entrante	Uso del puerto
Monitor de hardware de Streamvault	65116	Se utiliza para la comunicación HTTPS entre Security Center y el controlador de administración de la placa base iDRAC del hardware de Streamvault a través de la red.

Puertos requeridos del SV Control Panel

Los puertos de tráfico saliente que se enumeran a continuación deben abrirse para permitir que los componentes del Panel de control de Streamvault se conecten a los servicios en la nube de Genetec™.

Puerto de salida	Uso del puerto	URL de destino
TCP 443	Comunicación HTTPS con los servicios de respaldo de Genetec	svbackupservices.genetec.com genetecbackupservice.blob.core.windows.net

Puertos requeridos por CylancePROTECT

Los puertos de tráfico saliente que se enumeran a continuación deben abrirse para permitir que el agente de escritorio CylancePROTECT se comunique con la consola de administración de Genetec y reciba las actualizaciones del agente.

Puerto de salida	Uso del puerto	URL de destino
TCP 443	Comunicación HTTPS en América del Norte	cement.cylance.com data.cylance.com protect.cylance.com update.cylance.com api.cylance.com download.cylance.com venueapi.cylance.com

Puerto de salida	Uso del puerto	URL de destino
TCP 443	Comunicación HTTPS en el noreste de Asia y el Pacífico	cement-apne1.cylance.com data-apne1.cylance.com protect-apne1.cylance.com update-apne1.cylance.com api.cylance.com download.cylance.com venueapi-apne1.cylance.com
TCP 443	Comunicación HTTPS en el sudeste de Asia y el Pacífico	cement-au.cylance.com cement-apse2.cylance.com data-au.cylance.com protect-au.cylance.com update-au.cylance.com api.cylance.com download.cylance.com venueapi-au.cylance.com
TCP 443	Comunicación HTTPS en Europa Central	cement-euc1.cylance.com data-euc1.cylance.com protect-euc1.cylance.com update-euc1.cylance.com api.cylance.com download.cylance.com venueapi-euc1.cylance.com
TCP 443	Comunicación HTTPS en Sudamérica	cement-sae1.cylance.com data-sae1.cylance.com protect-sae1.cylance.com update-sae1.cylance.com api.cylance.com download.cylance.com venueapi-sae1.cylance.com
TCP 443	Comunicación HTTPS en GovCloud	cement.us.cylance.com data.us.cylance.com protect.us.cylance.com update.us.cylance.com api.us.cylance.com download.cylance.com download.us.cylance.com

Puerto de salida	Uso del puerto	URL de destino
		venueapi.us.cylance.com
TCP 443	Comunicación HTTPS para activar Cylance después de la reinstalación	svservices.genetec.com

NOTA: Si no desea abrir las conexiones salientes anteriores, se puede cambiar CylancePROTECT al modo desconectado. En modo desconectado, CylancePROTECT recibe actualizaciones del agente de Genetec™ Update Service (GUS).

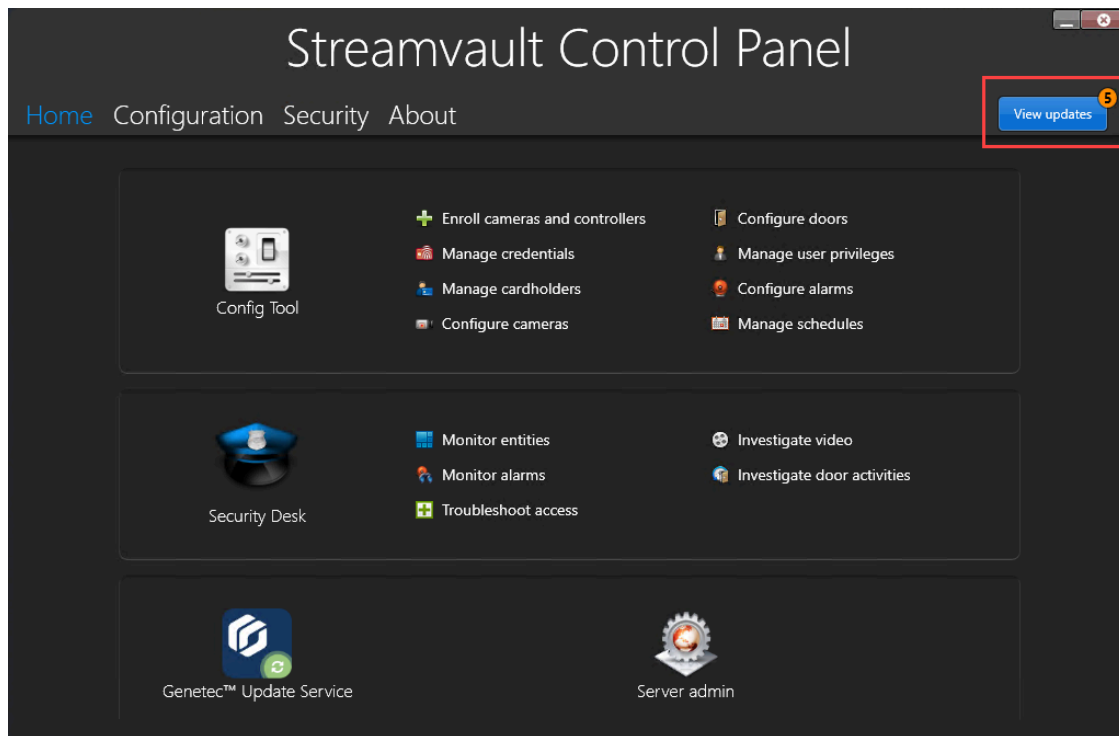
Para obtener más información sobre los modos en los que el dispositivo Streamvault se comunica con los servicios de administración de Genetec, consulte [Página de seguridad del SV Control Panel](#) en la página 74.

Acerca de la actualización del software de SV en el SV Control Panel

El Genetec™ Update Service (GUS) está integrado en el SV Control Panel para ayudar a garantizar que los componentes de software de su dispositivo estén actualizados.

Cuando haya actualizaciones disponibles, el **Ver actualizaciones** El botón se muestra con una insignia que indica cuántas actualizaciones hay disponibles. Si hace clic en el botón para **Ver actualizaciones**, se inicia el GUS en un navegador.

NOTA: El color de la indicación varía de acuerdo con la importancia de las actualizaciones. Una indicación de color naranja señala las actualizaciones recomendadas y una indicación roja, las actualizaciones críticas.



Las principales características de GUS son las siguientes:

- Actualice sus productos Genetec™ cuando haya una nueva versión disponible.
- Busque actualizaciones a intervalos regulares.
- Configure las actualizaciones para que se descarguen en segundo plano, pero tendrá que instalarlas de manera manual.
- Vea cuándo se realizó la última búsqueda de actualizaciones.
- Actualiza de manera automática la licencia en segundo plano para garantizar que sea válida y que la fecha de vencimiento esté actualizada.
- Habilite varias funciones, como el Programa de mejora de Genetec.
- Revisa su firmware y recomienda actualizaciones o le notifica vulnerabilidades.

Para obtener más información sobre cómo utilizar GUS, consulte la [Guía del Usuario del Genetec™ Update Service](#) en el TechDoc Hub.

Conectar los componentes del dispositivo Streamvault

A fin de preparar su dispositivo Streamvault™ para el uso, debe conectar los periféricos requeridos (monitor, teclado y mouse), los periféricos opcionales, la red y una fuente de alimentación.

Antes de empezar

Despeja el espacio alrededor del botón de encendido. Para evitar apagar accidentalmente el aparato, asegúrese de que nada toque o esté demasiado cerca del botón de encendido.

Procedimiento

- 1 Conecte el cable del monitor de pantalla a una entrada de video compatible: conector VGA, HDMI o DisplayPort.
Al menos un monitor debe estar conectado al dispositivo. Puede conectar hasta tres monitores al mismo dispositivo.
- 2 Enchufe el monitor a un tomacorriente de CA y enciéndalo.
- 3 Conecte el teclado y el mouse a un puerto USB disponible.
- 4 (Opcional) Conecte los periféricos opcionales:
 - Oradores
 - [Cámaras analógicas](#)
 - [Entradas y salidas de alarma](#)
- 5 Conecte un cable Ethernet al puerto Ethernet del dispositivo. Conecte el otro extremo del cable al conector RJ-45 de la red IP.
- 6 Para los dispositivos Streamvault™ SV-100E, inserte el enchufe de CC en el conector de entrada de 19,5 V del dispositivo y el otro extremo en el bloque de la fuente de alimentación. Conecte el cable del bloque a una toma de corriente.
- 7 Para encender el dispositivo Streamvault, presione el botón de encendido.

Después de que concluya

[Inicie sesión en su dispositivo Streamvault.](#)

Tarjetas codificadoras analógicas de Genetec

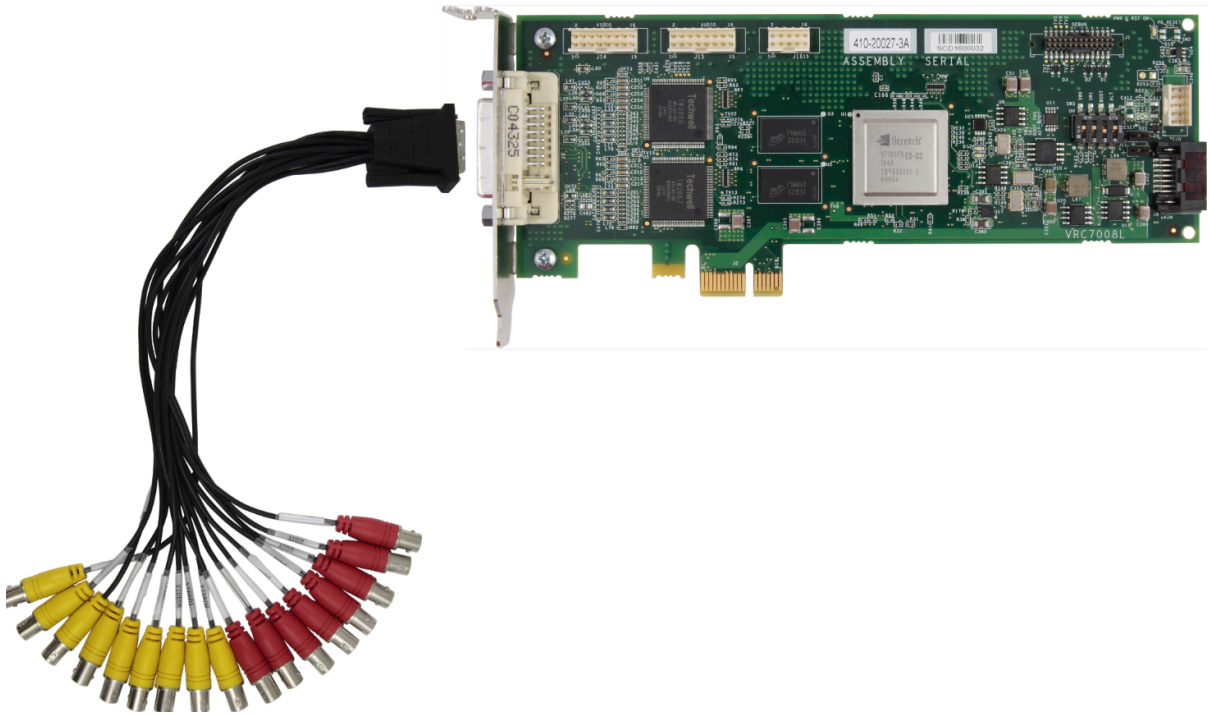
Si está usando un dispositivo Streamvault para implementar un sistema de administración de video con cámaras analógicas, debe conectar las cámaras a la tarjeta codificadora analógica de Genetec™ en el dispositivo.

Especificaciones de la tarjeta codificadora analógica

Se aplican las siguientes especificaciones a los dispositivos Streamvault que incluyen la tarjeta de video analógico:

- 8 o 16 entradas de video analógico, según la tarjeta que se instale
- Resolución de vídeo máxima 4CIF
- Cuadros máximos por segundo: 30 FPS
- Compatible con formato de compresión H.264

Limitación: Para que la tarjeta codificadora analógica pueda grabar, su dispositivo Streamvault debe tener una conexión de red. Si no hay una conexión de red disponible, debe configurar una interfaz de repetición para que la tarjeta codificadora funcione de manera adecuada.



Acerca de la conexión de cámaras analógicas

Si su dispositivo Streamvault incluye la tarjeta codificadora analógica de Genetec, este se envía con un cable de conexión con conectores BNC. Los conectores BNC se usan para conectar las cámaras analógicas de manera directa a la tarjeta codificadora incorporada.

Acerca de agregar cámaras analógicas en Security Center

Para agregar cámaras analógicas en Security Center, debe usar la herramienta de inscripción de la unidad. Para obtener más información, consulte [Acerca de la herramienta de inscripción de la unidad](#).

Considere lo siguiente al agregar cámaras analógicas:

- No puede agregar cámaras analógicas en Security Center usando el método de *Agregar de manera manual*. Use la herramienta de inscripción de la unidad.
- Para descubrir nuevas unidades y utilizar la herramienta de inscripción de la unidad, debe conectarse a Config Tool de manera local.
- Al seleccionar el fabricante de la cámara en la herramienta de inscripción de la unidad, puede encontrar todas las cámaras analógicas enumeradas en *Tarjeta codificadora Genetec* del fabricante.

Deshabilitar las entradas de cámara en tarjetas codificadoras en el dispositivo Streamvault

A fin de actualizar una licencia de conexión de cámara de analógica a IP, debe deshabilitar las entradas de cámara en la tarjeta codificadora.

Procedimiento

- 1 Desde la página de inicio de la herramienta de configuración, haga clic en *Acerca de* pestaña.

- 2 Haga clic en la pestaña de **Omnicast™** y verifique el número de cámaras que aparecen junto a *Número de cámaras y monitores analógicos..*
Por ejemplo: 16 / 16.
- 3 Abra la tarea de *Video*.
- 4 Desde el árbol de entidades, haga clic en la unidad de video que corresponde a la tarjeta codificadora.
- 5 Haga clic en la pestaña de **Periféricos** y seleccione las cámaras que necesita deshabilitar.
Puede seleccionar varias cámaras presionando Ctrl y haciendo clic en las cámaras.
- 6 En la parte inferior del *Periféricos* página, haga clic en el círculo rojo (●) para desactivar las cámaras y luego haga clic en **Aplicar**.
Las cámaras deshabilitadas aparecen en gris y se muestra un punto rojo a la izquierda de cada cámara deshabilitada en la lista.
- 7 Sobre el *Acerca de* página, verifique que el número de cámaras sea exacto.
Es posible que deba reiniciar Config Tool para actualizar la cantidad de cámaras.
NOTA: Si una cámara que ha deshabilitado grabó video, la cámara se muestra en el árbol de entidades en la tarea de *Monitorear* de Security Desk. Puede ver la reproducción desde esa cámara.

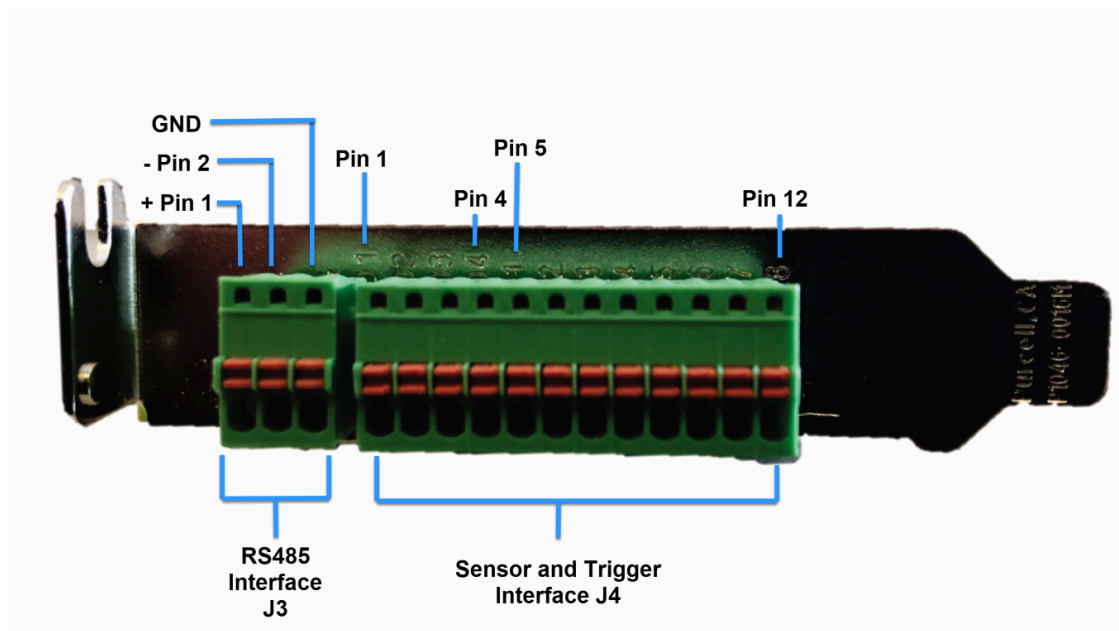
Entradas y salidas de alarma de un Streamvault aparato

Si está usando un Streamvault dispositivo para implementar un sistema de control de acceso, puede usar la tarjeta de E/S para conectar entradas de alarma de hardware de manera directa al dispositivo y luego controlar sus salidas mediante eventos a toma de acción en Security Center.

Especificaciones de la tarjeta de E/S

Se aplican las siguientes especificaciones a los modelos de Streamvault que incluyen la tarjeta de E/S:

- 4 salidas de activación
- 8 entradas de alarma
- Puerto de comunicaciones RS-485



Acerca de la conexión de entradas de E/S

Puede conectar los cables de entrada y salida de dispositivos de hardware de manera directa a la tarjeta de E/S en la parte posterior del Streamvault dispositivo. Los cables deben insertarse usando un pequeño destornillador de punta plana para empujar las abrazaderas de tensión en el conector.

Acerca de la creación de eventos a acciones

Para obtener información sobre cómo crear eventos a toma de acción para Streamvault, consulte [Crear eventos a toma de acción](#) en el TechDoc Hub.

Acerca de las cuentas de usuario de Streamvault

Hay dos tipos de cuentas de usuario de Streamvault™: administrador local y no administrador local. Dependiendo del tipo de cuenta de usuario con la que inicie sesión en SV Control Panel, verá solo las funciones que sean relevantes para usted.

Administrador local

La cuenta de usuario del administrador local (Admin) se crea de forma predeterminada. Una persona que inicia sesión como Administrador tiene derechos administrativos completos en SV Control Panel. El Administrador puede configurar todos los ajustes relacionados con el sistema y la seguridad en SV Control Panel, y puede crear cuentas de usuario que no sean de administrador.

No administrador local

La cuenta de usuario local de no administrador predeterminada para dispositivos y estaciones de trabajo todo en uno es la cuenta de Operador. Si una persona inicia sesión como Operador, tiene acceso restringido a las funciones de SV Control Panel. El Operador puede iniciar Config Tool y Security Desk, ver información del sistema y las licencias y acceder a la documentación del producto.

Si una persona inicia sesión como Administrador puede crear otras cuentas que no sean de administrador, que también tienen acceso limitado a SV Control Panel.

NOTA: Es posible eliminar las restricciones de acceso predeterminadas impuestas a todas las cuentas de usuarios que no sean de administradores. Para obtener información sobre cómo hacerlo, consulte [Cómo eliminar restricciones de cuentas de usuarios que no son administradores](#) en la página 117.

Información de inicio de sesión para las cuentas de usuario predeterminadas en un dispositivo Streamvault

La primera vez que tu Streamvault se inicia el dispositivo, se crean las cuentas de usuario de administrador y operador de Windows. Estas cuentas tienen distintos derechos de acceso y contraseñas predeterminadas. El administrador del servidor también tiene una contraseña predeterminada.

Las siguientes contraseñas predeterminadas son para el inicio de sesión inicial. Durante la configuración, crea su propia contraseña para la Config Tool y Security Desk.

Nombre de usuario	Contraseña predeterminada	Acceso concedido a	Acceso denegado a
Administrador	administración	Acceso completo al sistema: <ul style="list-style-type: none"> Windows: todas las funciones administrativas y del sistema Security Center Panel de control SV 	No aplicable
Operador	operador	<ul style="list-style-type: none"> Papelera de reciclaje Bibliotecas Mi PC C: conducir Página de inicio de SV Control Panel, Página de 	<ul style="list-style-type: none"> Windows: apagar y reiniciar Configuración del sistema Partición de video

Nombre de usuario	Contraseña predeterminada	Acceso concedido a	Acceso denegado a
		Configuración, Solo ajustes regionales, Página Acerca de <ul style="list-style-type: none"> Administrador del servidor: requiere contraseña de administrador para tener todos los derechos 	
No aplica	genetecfactory	Administrador del servidor	NOTA: Esta opción no está disponible para dispositivos de estación de trabajo.

Para cambiar su cuenta de usuario de Windows, aplicación cliente o Server Admin, inicie sesión en SV Control Panel con su cuenta de usuario de Administrador de Windows. En la página de *Seguridad*, en la sección de *Credenciales*, puede administrar todas tus contraseñas.

NOTA: La cuenta de Operador no se crea con una plantilla. Si crea una nueva cuenta de usuario, no tendrá las mismas restricciones de forma predeterminada.

Administrador del servidor del Security Center

- Solo los usuarios Administradores pueden iniciar sesión en Server Admin.
- Para iniciar sesión desde su máquina local, haga clic en el **Administrador del servidor** acceso directo en su escritorio.
- Para iniciar sesión en Server Admin de manera remota, debe conocer el nombre DNS o la dirección IP del servidor, el puerto de Web Server y la contraseña del servidor. Cuando introduzca la contraseña predeterminada, se le solicitará que la cambie.

IMPORTANTE: Para garantizar la seguridad de su sistema, cambie inmediatamente todas las contraseñas predeterminadas. Use las mejores prácticas de la industria para crear contraseñas seguras.

Temas relacionados

[Modificación de GPO locales para cuentas de usuarios no administradores](#) en la página 123

Iniciar sesión en un Streamvault aparato

La primera vez que inicie su dispositivo Streamvault™, se le solicitará que cambie la contraseña de Administrador predeterminada. También cambie la contraseña de Operador predeterminada. Luego puede iniciar sesión como usuario operador o administrador.

Antes de empezar

Conozca qué derechos de acceso tienen las cuentas de Operador y Administrador.

Lo que debería saber

Inicie sesión como usuario Administrador para configurar su dispositivo en SV Control Panel.

IMPORTANTE: Las contraseñas deben cumplir los siguientes requisitos:

- Mínimo de 14 caracteres
La longitud mínima es de 10 caracteres para dispositivos con versiones de imagen que no tienen el servicio Streamvault. Para obtener información sobre qué dispositivos tienen el servicio Streamvault y cuáles no, consulte [Dispositivos con capacidades de administración de endurecimiento](#) en la página 16.
- Deben contener al menos tres caracteres de las siguientes cuatro categorías:
 - Letras en mayúscula
 - Letras en minúscula
 - 10 dígitos base (0 a 9)
 - Caracteres no alfanuméricos (como \$, %, !)

Procedimiento

- 1 Encienda el aparato.
- 2 Inicie sesión con el nombre de usuario del Administrador y la contraseña predeterminada que están impresos en el dispositivo.
- 3 Ingrese una nueva contraseña de administrador.
Ha iniciado sesión como usuario Administrador.
NOTA: Algunos modelos solo tienen la cuenta de administrador de forma predeterminada.
- 4 Cierre sesión, y luego vuelva a iniciarla con el nombre de usuario del Operador y la contraseña predeterminada impresos en el dispositivo.
- 5 Ingrese una nueva contraseña de operador.
Ha iniciado sesión como usuario Operador.
- 6 Continúe la sesión de Operador o cierre la sesión y vuelva a iniciarla como usuario Administrador.

Después de que concluya

[Inicie la configuración inicial de su dispositivo.](#)

Acerca del servicio Streamvault

El servicio Streamvault es un servicio de Windows que permite a los usuarios configurar un dispositivo Streamvault™, como por ejemplo aplicar perfiles de endurecimiento.

El servicio Streamvault puede aplicar los siguientes perfiles de endurecimiento en los dispositivos:

- Líneas de base de seguridad de Microsoft
- Líneas de base de seguridad de Microsoft con el perfil de Nivel 1 del Centro de Seguridad de Internet (CIS)
- Líneas de base de seguridad de Microsoft con el perfil CIS Nivel 2
- Líneas de base de seguridad de Microsoft con el perfil de la Guía de Implementación Técnica de Seguridad (STIG)

Consulte [Acerca del endurecimiento de Streamvault](#) en la página 16 para obtener más información sobre los perfiles de endurecimiento.

Cuando un usuario Administrador selecciona un perfil de endurecimiento en el SV Control Panel, el servicio Streamvault aplica el perfil al dispositivo.

Las actualizaciones para el servicio Streamvault están disponibles de manera periódica y se pueden aplicar a través de Genetec™ Update Service (GUS) o del Portal de Asistencia Técnica de Genetec (GTAP). Cuando hay una actualización disponible, aparece una notificación en el SV Control Panel. Instalar las actualizaciones es opcional pero se lo recomendamos para acceder a nuevas versiones de los perfiles de endurecimiento.

Acerca del endurecimiento de Streamvault

El endurecimiento mejora la seguridad de su dispositivo Streamvault™ al aplicar un conjunto específico de configuraciones de seguridad.

Al endurecer su dispositivo, lo está optimizando para obtener más seguridad, aunque es posible que sacrifique un poco de facilidad de uso o rendimiento. Cuánto endurezca su dispositivo depende de su modelo de amenaza y de la sensibilidad de su información.

El endurecimiento se aplica en la página de *Seguridad* del SV Control Panel. Hay cuatro perfiles de endurecimiento predefinidos para elegir.

De forma predeterminada, todos los dispositivos se envían con el perfil de endurecimiento de Microsoft con CIS Nivel 2 aplicado.

Perfil de endurecimiento	Descripción
Microsoft (solamente)	<p>Este perfil de endurecimiento aplica las líneas base de seguridad de Microsoft a su sistema. Las líneas de base de seguridad de Microsoft son un grupo de configuraciones recomendadas por Microsoft que se basan en los comentarios de los equipos de ingeniería de seguridad, grupos de productos, socios y clientes de Microsoft.</p> <p>Las líneas de base de Microsoft que se implementan en los dispositivos Streamvault son la línea de base de Windows y la línea de base de Microsoft Edge.</p>
Microsoft con CIS Nivel 1	<p>Este perfil de endurecimiento aplica las líneas de base de seguridad de Microsoft y el perfil de Nivel 1 (CIS L1) del Centro de seguridad de Internet (CIS) a su sistema. El CIS L1 proporciona requisitos de seguridad esenciales que se pueden implementar en cualquier sistema con poco o ningún impacto en el rendimiento o funcionalidad reducida.</p>
Microsoft con CIS Nivel 2	<p>Este perfil de endurecimiento aplica las líneas de base de seguridad de Microsoft y los perfiles CIS L1 y Nivel 2 (L2) a su sistema. El perfil CIS L2 ofrece el más alto nivel de seguridad y está destinado a organizaciones donde la seguridad es de suma importancia.</p> <p>La estricta seguridad que aporta este perfil de endurecimiento puede reducir la funcionalidad del sistema y dificultar la gestión remota del servidor.</p>
Microsoft con STIG	<p>Este perfil de endurecimiento aplica las líneas de base de seguridad de Microsoft y las Guías de implementación técnica de seguridad (STIG) de la Agencia de Sistemas de Información de Defensa (DISA) a su sistema. Los STIG de DISA se basan en los estándares del Instituto Nacional de Estándares y Tecnología (NIST) y brindan protección de seguridad avanzada para los sistemas Windows del Departamento de Defensa de los EE. UU.</p>

NOTA: Los perfiles de endurecimiento están disponibles solo en dispositivos que tengan [Servicio Streamvault](#). Para obtener más información, consulte [Acerca del servicio Streamvault](#) en la página 15.

Dispositivos con capacidades de administración de endurecimiento

Sólo aquellos dispositivos con el servicio Streamvault™ tienen capacidades de administración de endurecimiento. El tipo de dispositivo y la imagen determinan si el servicio Streamvault está disponible.

La siguiente tabla describe qué dispositivos tienen el servicio Streamvault y cuáles no.

Tipo de dispositivo	Versiones de imágenes con el servicio Streamvault	Versiones de imágenes sin el servicio Streamvault
Todo en uno	<ul style="list-style-type: none"> 11.2024.2 	<ul style="list-style-type: none"> 16 17 18 19
SVW	<ul style="list-style-type: none"> 11.2024.2 	<ul style="list-style-type: none"> 0010.4 0011.2 0012.2 0013.2
SVA	<ul style="list-style-type: none"> 11.2024.2 	<ul style="list-style-type: none"> 0010.4 0011.2 0012.2 0013.2
SVR	<ul style="list-style-type: none"> 10.2021.2 11.2024.2 	<ul style="list-style-type: none"> 0012.2.X
Otros dispositivos Streamvault	<ul style="list-style-type: none"> WS.2022.1 	<ul style="list-style-type: none"> 2016.1.B 2016.1.C 2019.1 2019.4.C 2022.1.C

NOTA: Para obtener información sobre cómo encontrar la versión de imagen de su dispositivo, consulte [Encontrar la ID del sistema y la versión de la imagen de un dispositivo Streamvault](#) en la página 89.

Introducción a SV Control Panel

La introducción presenta SV Control Panel y ofrece información sobre cómo configurar su sistema Streamvault.

Esta sección incluye los temas siguientes:

- ["Acerca del panel de control de SV"](#) en la página 19
- [" Activación de su licencia de Security Center en un dispositivo "](#) en la página 22
- [" Activar una licencia de manera manual desde el Server Admin "](#) en la página 24
- ["Activar System Availability Monitor"](#) en la página 26
- [" Habilidad de las características de control de acceso y video de Security Center "](#) en la página 27
- ["Acerca de la Herramienta de Inscripción de la Unidad"](#) en la página 30
- [" Configurar los ajustes predeterminados de la cámara "](#) en la página 33
- [" Crear horarios de grabación personalizados "](#) en la página 35
- [" Acerca de la copia de respaldo y la restauración "](#) en la página 36
- [" Elegir el método para crear funciones y particiones del Archiver "](#) en la página 39
- [" Cifrado de la unidad del SO "](#) en la página 44
- [" Recopilación de registros de soporte "](#) en la página 48

Acerca del panel de control de SV

El SV Control Panel es una aplicación de interfaz de usuario que puede utilizar para configurar su dispositivo Streamvault™ para que funcione con el control de acceso y la videovigilancia de Security Center.

PRECAUCIÓN: Los cambios de configuración que realice en el SV Control Panel sobrescriben los cambios de configuración realizados fuera del SV Control Panel, incluidas las configuraciones personalizadas de Windows.

SV Control Panel se puede ejecutar de las siguientes maneras:

- Modo de expansión para configuraciones que se ejecutan en un servidor de expansión.
- Modo Cliente para las configuraciones que se ejecutan en dispositivos de Estación de Trabajo.
- Modo Directory para las configuraciones que se ejecutan en el servidor primario.

SV Control Panel incluye las siguientes funciones:

- Asistente de *configuración de Streamvault Control Panel* para ayudarlo a configurar su dispositivo de manera rápida.
- Asistente de *activación de Streamvault Control Panel* para ayudar a activar su dispositivo.
- Asistente de *instalación de Security Center* que puede usar para configurar Security Center.
- Asistentes de *Copia de respaldo de Streamvault Control Panel* y *Restauración de Streamvault Control Panel* para ayudar a crear copias de respaldo de la base de datos y las configuraciones de su Directory y restaurar estos archivos a su sistema en caso de ser necesario.
- Genetec™ Update Service (GUS), que verifica con regularidad si hay actualizaciones de software.
- Accesos directos para las tareas de uso frecuente en Config Tool y Security Desk.
- Enlaces al Portal de Asistencia Técnica de Genetec (GTAP) y a la documentación del producto.
- La opción de elegir el modo de operación del software antivirus Cylance provisto con su dispositivo Streamvault™. Las opciones se enumeran en la página de configuración de *Seguridad*.
- La capacidad de crear particiones y funciones adicionales del Archiver para las configuraciones de los servidores de expansión.

NOTA:

- Esta guía es aplicable a la versión 3.2.1 del SV Control Panel, que puede descargar desde GTAP.
- Las versiones de SV Control Panel a partir de 3.0 son compatibles con los dispositivos que no tienen el servicio Streamvault. Sin embargo, estos dispositivos no tienen acceso a los perfiles de endurecimiento.

Configuración de su dispositivo en SV Control Panel

La primera vez que inicia sesión en su dispositivo Streamvault™, el Panel de control de SV abre la ventana *Configuración del panel de control de Streamvault* asistente para guiarlo a través de la configuración inicial.

Antes de empezar

Conecte el aparato a Internet.

Lo que debería saber


- La configuración aplicada en el asistente se podrá cambiar más adelante desde la página de *Configuración* de SV Control Panel.
- Para el Archiver, las analíticas, la estación de trabajo o cualquier otro dispositivo que sea un servidor de expansión de Security Center, no se le solicitará que cambie las contraseñas de usuario.

Procedimiento

- 1 Encienda su electrodoméstico.

SV Control Panel inicia con el asistente de *configuración de Streamvault Control Panel* abierto.

NOTA: SV Control Panel solo se abre de manera automática la primera vez que se enciende el dispositivo. Cuando vuelva a prenderlo, los usuarios deben iniciar sesión con sus credenciales de administrador e iniciar el SV Control Panel.

- 2 Sobre el *Introducción* página, haga clic **Próximo**.
- 3 En la página de *Red*, configure los ajustes de la conexión IP:
 - a) Si utiliza DHCP para obtener una IP de manera automática (predeterminado) y falta la dirección IP, haga clic en **Actualizar**  para obtener una nueva dirección IP. Luego haga clic en **Reintentar**.
 - b) Si el campo de **Estado** muestra algo diferente a "Conectado a internet", haga clic en **Reintentar**.
 - c) Cuando el campo de **Estado** muestre "Conectado a internet", haga clic en **Siguiente**.
- 4 En la página de *Configuración de la computadora*, complete los campos en las secciones de *Información general* y *Configuración regional*.
- 5 Para cambiar la interfaz de usuario a otro idioma:
 - a) De **Idioma del producto**, Elige tu idioma.
 - b) Reinicie el SV Control Panel.
 - c) Cuando el asistente de *Configuración del Panel de Control de Streamvault* se vuelva a abrir, haga clic en **Siguiente** en la página de *Configuración de la computadora*.
- 6 Sobre el *Configurar CylancePROTECT* página, elija un modo de comunicación:
 - **En línea (recomendado):** Cuando está en línea, el Agente de CylancePROTECT se comunica con Genetec para informar sobre nuevas amenazas, actualizar su agente y enviar datos para ayudar a mejorar sus modelos matemáticos. Esta opción ofrece el más alto nivel de protección.
 - **Desconectado:** El modo de desconexión es para un dispositivo sin conexión a internet. En este modo, CylancePROTECT no puede conectarse ni enviar información a los servicios de gestión de Genetec en la nube. Su dispositivo está protegido contra la mayoría de las amenazas. El mantenimiento y las actualizaciones están disponibles a través de Genetec™ Update Service (GUS).
 - **Desactivar:** Seleccione este modo para desinstalar CylancePROTECT de manera permanente de su dispositivo. Su dispositivo utilizará Microsoft Defender para la protección y detección de amenazas de Windows. No recomendamos desactivar CylancePROTECT si el dispositivo no puede recibir actualizaciones de definiciones de virus para Microsoft Defender.
- 7 Haga clic en **Habilitar la administración de cuarentena** para agregar capacidades adicionales al ícono de Cylance en la barra de tareas, incluida la opción de **Eliminar cuarentena** para eliminar los archivos que Cylance ha puesto en cuarentena.
- 8 En la página de *Credenciales*, haga clic en **Modificar contraseña** para configurar las contraseñas para las siguientes aplicaciones:
 - **Security Center (Usuario administrador):** La contraseña del usuario administrador para Security Desk, Config Tool y Genetec™ Update Service.
 - **Administrador del servidor:** La contraseña para la aplicación Genetec™ Server Admin.

No se le solicitará que cambie las contraseñas en un dispositivo que es un servidor de expansión de Security Center. Seleccione **Saltar este paso** si no desea establecer contraseñas nuevas.
- 9 En la página de *Endurecimiento*, seleccione uno de los siguientes perfiles de endurecimiento:
 - **Microsoft (solamente):** Este perfil de endurecimiento aplica las líneas base de seguridad de Microsoft a su sistema. Las líneas de base de seguridad de Microsoft son un grupo de configuraciones recomendadas por Microsoft que se basan en los comentarios de los equipos de ingeniería de seguridad, grupos de productos, socios y clientes de Microsoft.
 - **Microsoft con CIS Nivel 1:** Este perfil de endurecimiento aplica las líneas de base de seguridad de Microsoft y el perfil de Nivel 1 (CIS L1) del Centro de seguridad de Internet (CIS) a su sistema. El CIS L1

proporciona requisitos de seguridad esenciales que se pueden implementar en cualquier sistema con poco o ningún impacto en el rendimiento o funcionalidad reducida.

- **Microsoft con CIS Nivel 2:** Este perfil de endurecimiento aplica las líneas de base de seguridad de Microsoft y los perfiles CIS L1 y Nivel 2 (L2) a su sistema. El perfil CIS L2 ofrece el más alto nivel de seguridad y está destinado a organizaciones donde la seguridad es de suma importancia.
NOTA: La estricta seguridad que aporta este perfil de endurecimiento puede reducir la funcionalidad del sistema y dificultar la gestión remota del servidor.
- **Microsoft con STIG:** Este perfil de endurecimiento aplica las líneas de base de seguridad de Microsoft y las Guías de implementación técnica de seguridad (STIG) de la Agencia de Sistemas de Información de Defensa (DISA) a su sistema. Los STIG de DISA se basan en los estándares del Instituto Nacional de Estándares y Tecnología (NIST) y brindan protección de seguridad avanzada para los sistemas Windows del Departamento de Defensa de los EE. UU.

NOTA: La página de *Endurecimiento* está disponible solo para los dispositivos con el servicio Streamvault.

10 En la página del *System Availability Monitor*, elija un método de recopilación de datos:

- **No recopilar datos:** El System Availability Monitor Agent está instalado pero no recopila ningún dato.
- **Los datos se recogerán de forma anónima.:** No se requiere código de activación. Los datos de estado se envían a un Servicio de Monitoreo del Estado de Salud en los que los nombres de las entidades se ocultan y no se pueden rastrear. Genetec Inc. solo usa estos datos para estadísticas y no se puede acceder a ellos a través de GTAP.
- **Los datos serán recopilados y vinculados a mi sistema.:** Se requiere un código de activación. Los datos del estado de salud que se recopilan se vinculan a un sistema que está registrado con un Acuerdo de Mantenimiento del Sistema (SMA, por sus siglas en inglés) activo.

11 Lea el acuerdo de confidencialidad, seleccione el cuadro de verificación **Acepto los términos del acuerdo de confidencialidad** y haga clic en **Aplicar**.

12 En la página de *Conclusión*, haga clic en **Cerrar**.

La opción **Iniciar el asistente de activación después de la configuración** está seleccionada de manera predeterminada. Si lo borra, se le recordará que active el producto.

Después de que concluya

[Active su dispositivo](#) antes de usarlo.

Activación de su licencia de Security Center en un dispositivo

El *Activación del panel de control de Streamvault* El asistente le ayuda a activar su licencia de Security Center en su dispositivo Streamvault™.

Antes de empezar

- Conecte su electrodoméstico a Internet.
- Asegúrese de tener la ID del Sistema y la contraseña que se le envió después de que compró la licencia.

Lo que debería saber

- Esta tarea solo se aplica a dispositivos con conexión a Internet. Para un dispositivo sin Internet, [active la licencia de Security Center de forma manual desde Server Admin](#).
- Solo necesita activar la licencia de Security Center en el dispositivo que aloja la función de Directory, no en el servidor de expansión ni en los dispositivos de la estación de trabajo.

Procedimiento

- 1 Desde el Panel de control de SV, haga clic en **El sistema no está activado. Haga clic aquí para activar**. Se abre el asistente de *activación de Streamvault Control Panel*.
NOTA: Si ve el mensaje *Se requiere acceso a Internet para la activación*, su dispositivo no está conectado a Internet. Conecte su dispositivo ahora o active su licencia de manera manual desde Server Admin.
- 2 En la página de *Activación*, haga clic en **ID del Sistema** y haga clic en **Siguiente**.
- 3 En la página de *ID del Sistema*, introduzca la ID del Sistema y la contraseña y haga clic en **Siguiente**.
- 4 En la página de *Resumen*, verifique que la ID del Sistema sea correcto y haga clic en **Activar**. Se abre la página de *Resultado*, que indica si la activación fue exitosa.
- 5 Haga clic en **Siguiente**.
- 6 (Opcional) En el *Actualizaciones* página, realice una de las siguientes acciones:
 - Si no hay actualizaciones disponibles, haga clic en **Abrir el asistente de instalación de Security Center**.
 - Si hay actualizaciones disponibles, haga clic en **Ver actualizaciones** para abrir Genetec™ Update Service e instalar las actualizaciones.
 - Si la verificación de actualización falló porque el directorio no responde, haga clic en **Abrir administrador del servidor** y asegúrese de que el Directorio esté listo.**NOTA:** Si Genetec Update Service no está listo, la búsqueda de actualizaciones podría fallar. Ve el mensaje *No se pueden buscar actualizaciones en este momento. Lo intentaremos de nuevo más tarde*.
- 7 En la página de *Características adicionales*, habilite o deshabilite Synergis™ Software y Genetec™ Mobile. Estas funciones solo se muestran si están instaladas en su electrodoméstico. La característica de Genetec Mobile solo está disponible para Security Center 5.8 y versiones anteriores.
- 8 Cierre el asistente de *activación de Streamvault Control Panel*.

Después de que concluya

- (Opcional) [Activar el agente del Monitor de disponibilidad del sistema](#).
- [Configure sus ajustes de Security Center usando el asistente de instalación de Security Center](#)

Temas relacionados

[Activar una licencia de manera manual desde el Server Admin](#) en la página 24

[Acerca de la página de SV Control Panel](#) en la página 78

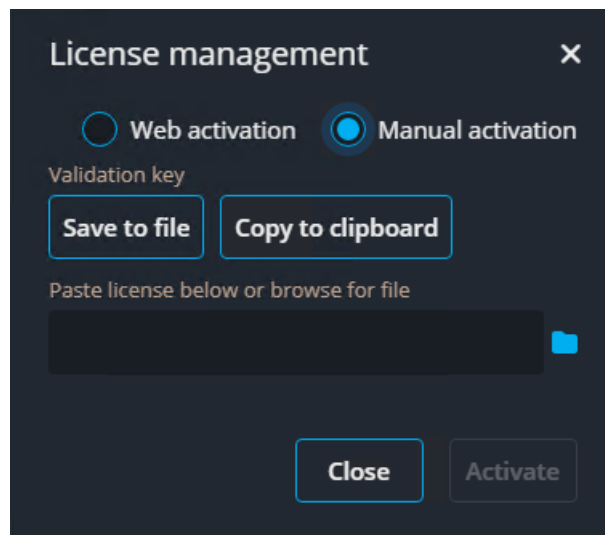
Activar una licencia de manera manual desde el Server Admin

Si su dispositivo Streamvault™ no tiene acceso a Internet, debe activar su licencia de Security Center de manera manual desde Server Admin.

Procedimiento

- 1 Guarde la clave de validación:
 - a) Desde su dispositivo, abra SV Control Panel.
 - b) Desde la página de inicio, haga clic en el ícono de **Server Admin**.
 - c) Inicie sesión en Administrador del servidor.
Si su contraseña de Server Admin es diferente de la contraseña del administrador de Windows, inicie sesión en Server Admin usando las credenciales de contraseña especificadas en el asistente de *configuración de Streamvault Control Panel*.
 - d) En la página de *Licencia*, haga clic en **Modificar**.
 - e) En el cuadro de diálogo de *Administración de licencias*, seleccione **Activación manual** > **Guardar en archivo**.

El nombre predeterminado para el archivo es *validación.vk*.



- f) Copia el *validación.vk* archivo a una llave USB.
 - g) Ejecute la memoria USB desde la computadora.

- 2 Obtenga la licencia del Portal de Asistencia Técnica de Genetec™ (GTAP, por sus siglas en inglés):
 - a) En otra computadora que tenga acceso a Internet, conecte la llave USB.
 - b) Iniciar sesión en [GTAP](#).
 - c) En la página de *Inicio de sesión del GTAP*, introduzca la ID del Sistema y la contraseña que se le asignó cuando adquirió la licencia y, a continuación, haga clic en **Inicio de sesión**.
 - d) Desde la página de *Información del sistema*, haga clic en **Activar licencia** en la sección de *Información de la licencia*.
 - e) En el cuadro de diálogo que se abre, pegue la clave de validación o busque el archivo.
 - f) En el cuadro de diálogo de *Activación*, busque el archivo *validation.vk* en la memoria USB y, a continuación, haga clic en **Enviar**.
Aparece el mensaje *Su licencia se activó de manera exitosa*.
 - g) Haga clic en **Descargar Licencia** y, a continuación, guarde la clave de licencia.
El nombre de archivo predeterminado es su ID del Sistema seguido de *_Directory_License.lic*.
 - h) Copie el archivo *_Directory_License.lic* en la memoria USB.
 - i) Ejecute la memoria USB desde la computadora.
- 3 Active su licencia:
 - a) En su electrodoméstico, conecte la llave USB.
 - b) Regrese a Server Admin.
 - c) En la página de *Licencia*, haga clic en **Modificar**.
 - d) En el cuadro de diálogo de *Administración de licencias*, seleccione **Activación manual**.
 - e) Pegue la información de la licencia desde el archivo *License.lic* (ábralo con un editor de texto) o busque el archivo *License.lic* y, a continuación, haga clic en **Abrir**.
 - f) Haga clic en **Activar**.

Temas relacionados

[Activación de su licencia de Security Center en un dispositivo](#) en la página 22

Activar System Availability Monitor

Para monitorear la disponibilidad de su sistema y los problemas de salud en GTAP, puede configurar System Availability Monitor para recopilar los datos sobre su dispositivo y enviarlos a los Servicios de Monitoreo de Salud.

Antes de empezar

Para recopilar y reportar información de salud sobre su dispositivo, debe generar un código de activación en GTAP. Para obtener información sobre cómo hacerlo, consulte [Generación de códigos de activación para el System Availability Monitor Agent](#) en el TechDoc Hub.

Procedimiento

- 1 Abra el Panel de control de SV.
- 2 En la página de *Configuración*, haga clic en **Configurar** en la sección *System Availability Monitor*.
- 3 En la ventana del *System Availability Monitor Agent*, haga clic en **Modificar**.
- 4 Verifique que el cuadro de verificación de **Los datos se recopilarán y enlazarán a mi sistema** esté seleccionado.
- 5 En el campo de **Código de activación**, escriba el código de su dispositivo.
- 6 Haga clic en **Aceptar**.

Habilitación de las características de control de acceso y video de Security Center

El *Asistente instalador de Security Center* lo guía a través de la configuración de las características principales de administración de video y control de acceso.

Lo que debería saber

Las configuraciones que aplique en el asistente se pueden cambiar más adelante en Config Tool.

Se aplica a: Los dispositivos que alojan la función de Directory, como dispositivos todo en uno.

Procedimiento

- 1 Inicie sesión como usuario administrador.

SUGERENCIA: Si su contraseña de Security Center es diferente de la contraseña de administrador de Windows, inicie sesión en Security Center utilizando las credenciales de contraseña especificadas en el *Configuración del panel de control de Streamvault* mago.

Se abre el asistente de instalación de Security Center.

- 2 Después de leer el *Introducción* página, haga clic **Próximo**.

- 3 En la página *Funciones disponibles*, elija las funciones que desee y haga clic en **Siguiente**.

De manera predeterminada, las características básicas están habilitadas. Puede habilitar y deshabilitar funciones más adelante en el *Características* página en el **Configuración general** vista de *Sistema* tarea.

NOTA: Si su licencia no admite una característica, esta no aparece en la lista.

- 4 En la página de *Seguridad de la cámara*, especifique el nombre de usuario y la contraseña predeterminados que usa para todas sus cámaras y luego haga clic en **Siguiente**.

SUGERENCIA: Para mayor seguridad, seleccione **Usar HTTPS**.

- 5 En la página de *Configuración de la calidad de la cámara*, configure las siguientes opciones:

- **Resolución:**
 - **Alta:** 1280x720 y superior
 - **Estándar:** más que 320x240 y menos que 1280x720
 - **Baja:** 320x240 e inferior
 - **Predeterminada:** configuración predeterminada del fabricante

La cámara siempre utiliza la resolución más alta que puede admitir de la categoría elegida. Si la cámara no admite ninguna de las resoluciones de la categoría elegida, usará la resolución más alta que pueda admitir de la siguiente categoría. Por ejemplo, si la cámara no puede admitir una resolución Alta, utiliza la resolución más alta que admite del grupo Estándar.

Los ajustes de esta página se pueden modificar más adelante desde la página de *Configuración predeterminada de la cámara* de la función de Archiver.

- 6 En la página de *Configuración de grabación*, seleccione la configuración predeterminada de grabación que desea aplicar a todas las cámaras.

- **Apagado:** La grabación está apagada.
- **Continuo:** Las cámaras graban de manera continua. Esta es la configuración predeterminada.
- **En movimiento / Manual:** Las cámaras graban cuando una acción (como Empezar a grabar, Agregar marcador o Activar alarma) las activa mediante la detección de movimientos o cuando un usuario lo indica de manera manual.
- **Registro de salida:** Las cámaras graban cuando una acción (como Empezar a grabar, Agregar marcador o Activar alarma) las activa o cuando un usuario lo indica de manera manual.

NOTA: Cuando se usa la opción **Manual**, el movimiento no activa ninguna grabación.

- **Personalizado:** Puede establecer un horario para cuando se produzca la grabación.

7 Hacer clic en **Siguiente**.

8 En la página de *Seguridad de la unidad del control de acceso*, especifique el nombre de usuario y la contraseña predeterminados para todas sus unidades del control de acceso y haga clic en **Siguiente**.

9 En la página de *Tarjetahabientes*, seleccione cómo desea agregar sus credenciales (tarjetas) y tarjetahabientes.

a) Seleccione si desea agregar tarjetahabientes (cuando se cierre el asistente de instalación de Security Center) a través de la tarea de *Administración de tarjetahabientes* o usando Import tool.

b) Hacer clic en **Siguiente**.


10 En la página de *Usuarios*, agregue más usuarios a su sistema:

a) Introduzca el nombre de usuario.

b) Seleccione el **Tipo de Usuario**:

- **Operador:** Un operador puede usar la tarea de *Monitorear*, ver videos y administrar visitantes en Security Desk.
- **Informes:** Un usuario de informes puede usar la aplicación Security Desk y ejecutar las tareas de informes más básicas, sin incluir las tareas para AutoVu™ ALPR. Un usuario que solo tiene privilegios de informar no puede ver los videos, controlar los dispositivos físicos ni informar incidentes.
- **Investigador:** Un investigador puede usar la tarea de *Monitorear*, ver videos, controlar cámaras PTZ, grabar y exportar videos, agregar marcadores e incidentes, usar tareas de investigación, administrar alarmas y visitantes, anular horarios de desbloqueo de puertas, guardar tareas y demás.
- **Supervisor:** Un supervisor puede usar la tarea de *Monitorear*, ver videos, controlar cámaras PTZ, grabar y exportar videos, agregar marcadores e incidentes, usar tareas de investigación, administrar alarmas y visitantes, anular horarios de desbloqueo de puertas, guardar tareas y demás. Un supervisor también puede usar las tareas de mantenimiento, administrar los tarjetahabientes y credenciales, modificar los campos personalizados, establecer niveles de amenaza, bloquear cámaras y realizar conteo de personas.
- **Aprovisionamiento:** Un usuario de aprovisionamiento tiene la mayoría de los privilegios de configuración, excepto los siguientes: administrar funciones, macros, usuarios, grupos de usuarios, eventos personalizados, registros de actividades, niveles de amenaza y archivos de audio. El usuario de aprovisionamiento suele ser un instalador del sistema.
- **Operador básico de AutoVu:** Este tipo de usuario es para operadores que utilizan el ALPR de AutoVu. El usuario básico de AutoVu puede usar tareas de ALPR, configurar entidades de ALPR, crear reglas de ALPR, monitorear eventos de ALPR, etc.
- **Usuario patrullero:** Este tipo de usuario es para usuarios de Genetec Patroller™ que usen el ALPR de AutoVu. El usuario de Patroller básico puede usar tareas ALPR, configurar entidades ALPR, crear reglas ALPR, monitorear eventos ALPR, etc. Un usuario de Patroller no tiene acceso a otras aplicaciones de Security Center, por ejemplo, Config Tool y Security Desk. El usuario de Patroller no puede modificar los informes ni cambiar la contraseña de Patroller.

11 Introduzca y confirme la **Contraseña** y, a continuación, haga clic en **Agregar**.

Se agrega el usuario nuevo a la lista de usuarios a la derecha del cuadro de diálogo. Para eliminar un usuario, seleccione un usuario de la lista y haga clic en .

Cambia los perfiles de usuario en la vista de **Usuarios** de la tarea de *Administración de Usuarios*. Para obtener información, consulte la [Guía del administrador de Security Center](#) en el TechDoc Hub.

12 Hacer clic en **Siguiente**.

13 Confirme que la información de la página de *Resumen* sea correcta y, luego, haga clic en **Aplicar** o haga clic en **Atrás** para corregir los errores.

14 Sobre el *Conclusión* página, haga clic **Reanudar**.

Config Tool se reinicia para aplicar los ajustes.

NOTA: La opción de **Abrir la herramienta de inscripción de la unidad después de que el asistente se cierre** está seleccionada de manera predeterminada. Puede borrar esta opción y abrir la herramienta de inscripción de la unidad más tarde haciendo clic en el acceso directo de **Registrar cámaras y controladores** en la página de *Inicio* del SV Control Panel.

Después de que concluya

[Agregue unidades a su sistema](#) mediante el uso de la herramienta de inscripción de la unidad.

Temas relacionados

[Configurar los ajustes predeterminados de la cámara](#) en la página 33

[Crear horarios de grabación personalizados](#) en la página 35

[Página de inicio de SV Control Panel](#) en la página 69

Acerca de la Herramienta de Inscripción de la Unidad

La inscripción de unidades es una herramienta que puede utilizar para descubrir unidades IP (video y control de acceso) conectadas a su red, según el fabricante y las propiedades de la red (puerto de detección, rango de direcciones IP, contraseña, etc.). Después de detectar una unidad, puede agregarla a su sistema.

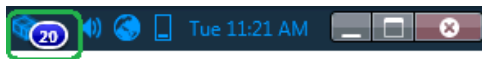
- La herramienta de registro de unidades se abre automáticamente después de la *Asistente de instalación de Security Center* a menos que hayas borrado el **Abra la herramienta de inscripción de unidades después del asistente** opción.
- Al agregar unidades de control de acceso, solo las unidades HID y Synergis™ se pueden inscribir con la Herramienta de inscripción de la unidad. Para obtener detalles completos sobre cómo inscribir unidades Synergis, consulte la *Guía de Configuración de Dispositivos Synergis™*.

Abrir la Herramienta de inscripción de la Unidad

Hay tres formas de abrir la herramienta de inscripción de la Unidad.

Procedimiento

- Realice una de las siguientes acciones:
 - Desde la página de inicio de SV Control Panel, haga clic en **+ Inscribir cámaras y controladores**.
 - Desde la página de Inicio del SV Control Panel, haga clic en el ícono de **Config Tool** y luego haga clic en **Tareas > Inscripción de unidades**.
 - Desde la página de Inicio del SV Control Panel, haga clic en el ícono de **Config Tool** y luego haga clic en el ícono de **Agregar estado de la unidad** en la bandeja de notificación de Config Tool.




Configurar los ajustes de inscripción de la unidad

Puede usar el botón de **Configuración y fabricantes** en la Herramienta de inscripción de la unidad para especificar qué fabricantes incluir al buscar unidades nuevas. También puede configurar los ajustes de descubrimiento para las unidades y especificar el nombre de usuario y las contraseñas para las unidades para que puedan inscribirse fácilmente.

Procedimiento


- 1 Desde la página de inicio, haga clic en **Herramientas > Inscripción de la unidad**.
- 2 En el *Matriculación de la unidad* cuadro de diálogo, haga clic en **Configuraciones y fabricantes** ()
- 3 Use la opción de **Rechazar la autenticación básica** para habilitar o deshabilitar la autenticación básica (solo unidades de video). Esto es útil si desactivó la autenticación básica en InstallShield de Security Center, pero necesita volver a activarla para realizar una actualización de firmware o para inscribir una cámara que solo admita la autenticación básica. Para volver a activar la autenticación básica, debe activar la opción de **Rechazar la autenticación básica** a **APAGADO**.
NOTA: Esta opción sólo está disponible para usuarios con privilegios de Administrador.
- 4 Haga clic en **Agregar fabricante** (+) para agregar un fabricante a la lista de unidades que se descubrirán.
 Para eliminar un fabricante de la lista, selecciónelo y haga clic en ✖.

- 5 Configure los ajustes individuales para cualquier fabricante que haya agregado. Para hacer esto, seleccione el fabricante y haga clic en  .
IMPORTANTE: Debe ingresar el nombre de usuario y la contraseña correctos para que la unidad se inscriba correctamente.
- 6 (Opcional) Eliminar unidades de la lista de unidades ignoradas (ver [Eliminar unidades de la lista de unidades ignoradas](#) en la página 32)
- 7 Haga clic en **Guardar** .

Agregar unidades

Una vez que se han descubierto unidades nuevas, puede usar la Herramienta de inscripción de la unidad para agregarlas a su sistema.

Procedimiento

- 1 Desde la página de inicio, haga clic en **Herramientas > Inscripción de la unidad**.
- 2 Hay tres formas de agregar unidades recién descubiertas:
 - Agregue todas las nuevas unidades descubiertas al mismo tiempo haciendo clic en **Agregar todo** () en la parte inferior derecha del cuadro de diálogo.
 - Haga clic en una sola unidad en la lista, luego haga clic en **Agregar** en la columna de **Estado**
 - Haga clic con el botón derecho en una sola unidad de la lista y haga clic en **Agregar o Agregar unidad** .

Cuando una unidad de video no tiene el nombre de usuario y la contraseña correctos, el **Estado** de la unidad aparecerá como **Inicio de sesión incorrecto** y se le pedirá que ingrese la información correcta cuando agregue la unidad. Si desea utilizar el mismo nombre de usuario y contraseña para todas las cámaras de su sistema, seleccione la opción **Guardar como autenticación predeterminada para todos los fabricantes** .

Además, puede agregar una unidad de manera manual haciendo clic en el botón de **Adición manual** en la parte inferior del cuadro de diálogo de la *Herramienta de inscripción de la unidad*.

NOTA:

- Para las unidades de video, si la cámara agregada es un codificador con múltiples transmisiones disponibles, cada transmisión se agrega con la *Cámara - n* cadena agregada al nombre de la cámara, *n* representando el número de transmisión. Para una cámara IP con solo una transmisión disponible, el nombre de la cámara no se modifica.
- Si está agregando un SharpV, de forma predeterminada, las unidades de cámara incluyen un certificado autofirmado que utiliza el nombre común de SharpV (por ejemplo, SharpV12345). Para agregar el SharpV al Archiver, debe generar un nuevo certificado (firmado o autofirmado) que use la dirección IP de la cámara en lugar del nombre común.

Borrar unidades agregadas

Puede borrar unidades que ya se han agregado a su sistema para que no se muestren cada vez que usa la Herramienta de inscripción de la unidad para descubrir unidades en su sistema.

Lo que debería saber

La opción de **Borrar completado** en la Herramienta de inscripción de la unidad es permanente, no se puede revertir.

Procedimiento

- 1 Agregue las unidades descubiertas deseadas a su sistema, vea [Agregar unidades](#) en la página 31 .
- 2 Una vez que se hayan agregado las unidades, haga clic en **Borrar completado** .
Cualquier unidad que se haya **agregado** en la columna **Estado** se borrará de la lista de unidades descubiertas.

Ignorando unidades

Puede escoger ignorar unidades para que no aparezcan en la lista de unidades descubiertas de la Herramienta de inscripción de la unidad.



Procedimiento

- 1 Desde la página de inicio, haga clic en **Herramientas > Inscripción de la unidad**.
Se abre la herramienta de inscripción de la unidad con la lista de las unidades que se han descubierto en el sistema.
- 2 Haga clic con el botón derecho en la unidad que desea ignorar y seleccione **Ignorar** .
La unidad se elimina de la lista y se ignorará cuando la herramienta de inscripción de la unidad descubra nuevas unidades. Para obtener información sobre cómo eliminar una unidad de la lista de unidades ignoradas, consulte [Eliminar unidades de la lista de unidades ignoradas](#) en la página 32 .

Eliminar unidades de la lista de unidades ignoradas

Puede eliminar una unidad de la lista de unidades ignoradas para que no se ignore cuando la Herramienta de inscripción de la unidad realiza un descubrimiento.

Procedimiento

- 1 Desde la página de inicio, haga clic en **Herramientas > Inscripción de la unidad**.
- 2 En la esquina superior derecha del cuadro de diálogo de *inscripción de Unidad* , haga clic en **Configuración y Fabricantes** ()
- 3 Haga clic **unidades ignorados** y haga clic en **Quitar todas las unidades ignorados**, o puede seleccionar una sola unidad y haga clic en el botón **Quitar unidad ignorado** ().

Configurar los ajustes predeterminados de la cámara

Desde el *Configuración predeterminada de la cámara*, puede modificar la configuración predeterminada de grabación y calidad de video aplicada a todas las cámaras controladas por Archiver. Inicialmente, estos ajustes se configuran en el *Configuración de calidad de la cámara* página en el asistente de instalación de Security Center.

Lo que debería saber

También puede aplicar configuraciones de video y grabación para una cámara en Config Tool usando el **Vídeo y grabación** pestaña de la unidad. Las configuraciones realizadas para una cámara individual tienen prioridad sobre las configuraciones que se aplican en el asistente de instalación de Security Center o en el *Configuración predeterminada de la cámara* página.

Procedimiento

- 1 Desde la página de inicio de Config Tool, abra el *Vídeo* tarea.
- 2 Seleccione la función Archiver y luego haga clic en **Configuración predeterminada de la cámara** pestaña.

- 3 En **Calidad de video (Igual en todos los archivos)**, configure lo siguiente:

- **Resolución:**
 - **Alta:** 1280x720 y superior
 - **Estándar:** más que 320x240 y menos que 1280x720
 - **Baja:** 320x240 e inferior
 - **Predeterminada:** configuración predeterminada del fabricante

La cámara siempre utiliza la resolución más alta que puede admitir de la categoría elegida. Si la cámara no admite ninguna de las resoluciones de la categoría elegida, usará la resolución más alta que pueda admitir de la siguiente categoría. Por ejemplo, si la cámara no puede admitir una resolución Alta, utiliza la resolución más alta que admite del grupo Estándar.

- 4 Bajo **Grabación**, haga clic  para agregar un horario.

Los horarios disponibles incluyen:

- Horarios que fueron creados usando la vista de **Horarios** en la tarea del *Sistema*.
- Un cronograma personalizado, si se creó uno en el asistente de instalación de Security Center.

- 5 Desde el **Modo** menú desplegable, seleccione un modo para el programa de grabación:

- **Apagado:** La grabación está apagada.
 - **Continuo:** Las cámaras graban de manera continua. Esta es la configuración predeterminada.
 - **En movimiento / Manual:** Las cámaras graban cuando una acción (como Empezar a grabar, Agregar marcador o Activar alarma) las activa mediante la detección de movimientos o cuando un usuario lo indica de manera manual.
 - **Registro de salida:** Las cámaras graban cuando una acción (como Empezar a grabar, Agregar marcador o Activar alarma) las activa o cuando un usuario lo indica de manera manual.
- NOTA:** Cuando se usa la opción **Manual**, el movimiento no activa ninguna grabación.
- **Personalizado:** Puede establecer un horario para cuando se produzca la grabación.

6 Configure las siguientes opciones:

- **Grabar audio:** Active esta opción cuando desee grabar un audio con video. Se debe asociar una entidad de micrófono a sus cámaras para que funcione esta opción.
- **Archivado redundante:** Active esta opción cuando desee archivar el video en los servidores primario y secundario al mismo tiempo. Esta configuración solo tiene efecto cuando se configura la conmutación por error.
- **Limpieza automática:** Active esta opción cuando desee eliminar un video después de una cantidad específica de días. El video se borra ya sea que el almacenamiento del Archiver esté lleno o no.
- **Tiempo para grabar antes de un evento:** Use el control deslizante para establecer la cantidad de segundos que desee grabar antes de un evento. Este búfer se guarda cada vez que comienza la grabación, lo que garantiza que todo lo que solicitó la grabación también se capture en video.
- **Tiempo para grabar después de una moción:** Establezca la cantidad de segundos durante los cuales desea continuar la grabación después de un evento de movimiento. Durante este tiempo, el usuario no puede detener la grabación.
- **Duración de grabación manual predeterminada :** Establezca la cantidad de minutos que desea grabar cuando un usuario inicia la grabación. El usuario puede detener la grabación en cualquier momento antes de que termine la duración establecida. Este valor también lo utiliza la acción Iniciar grabación, cuando se selecciona la duración de grabación predeterminada.

7 Hacer clic **Aplicar**.

8 Si desea aplicar los ajustes nuevos a todas las cámaras existentes, haga clic en **Sí**.


Temas relacionados


[Habilitación de las características de control de acceso y video de Security Center](#) en la página 27

Crear horarios de grabación personalizados

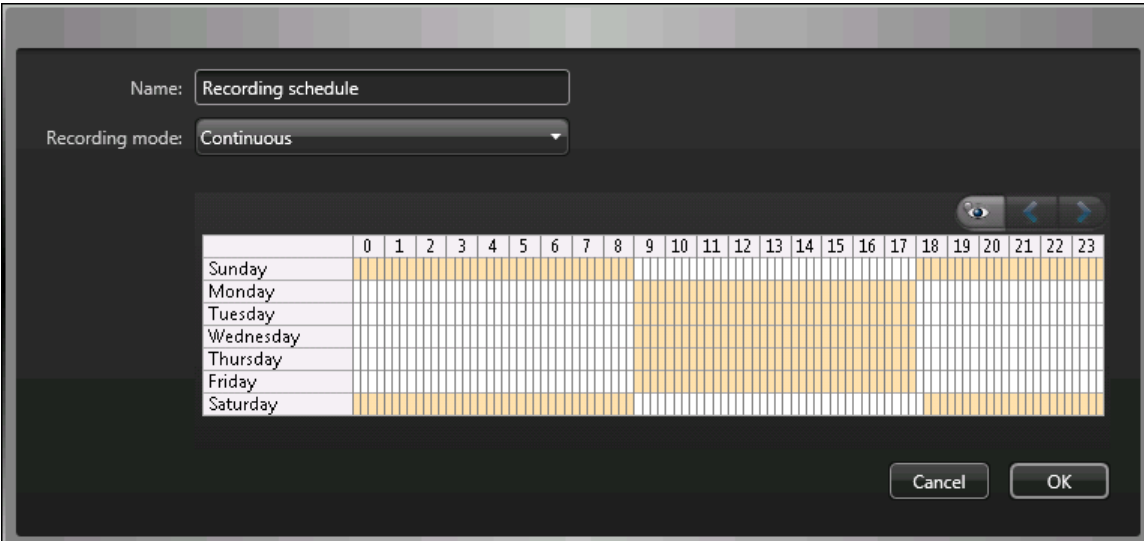
Cree horarios de grabación personalizados desde el asistente de instalación de Security Center para que las cámaras graben en diferentes modos de grabación durante un rango de tiempo específico.

Procedimiento

- 1 Sobre el *Configuración de grabación* página, haga clic  bajo **Horario de grabación**.
- 2 Introduzca un nombre para el horario nuevo.
- 3 En la lista **Modo de reproducción**, seleccione una de las siguientes opciones:
 - **Apagado:** La grabación está apagada.
 - **Continuo:** Las cámaras graban de manera continua. Esta es la configuración predeterminada.
 - **En movimiento / Manual:** Las cámaras graban cuando una acción (como Empezar a grabar, Agregar marcador o Activar alarma) las activa mediante la detección de movimientos o cuando un usuario lo indica de manera manual.
 - **Registro de salida:** Las cámaras graban cuando una acción (como Empezar a grabar, Agregar marcador o Activar alarma) las activa o cuando un usuario lo indica de manera manual.
- 4 Para cada día de la semana, especifique un rango de tiempo para la grabación:
 - Haga clic y arrastre para seleccionar un bloque de tiempo.
 - Haga clic derecho y arrastre para borrar un bloque de tiempo.
 - Use lasteclas del cursor para desplazarse por la cronología de 24 horas.

SUGERENCIA: Para cambiar al modo de alta resolución, donde cada bloque representa 1 minuto, haga clic en .

En el siguiente ejemplo, se muestra un horario en el que la grabación se realiza de manera continua de 6:00 p. m. a 9:00 a. m. los fines de semana y de 9:00 a. m. a 5:00 p. m. los días de semana.



Temas relacionados

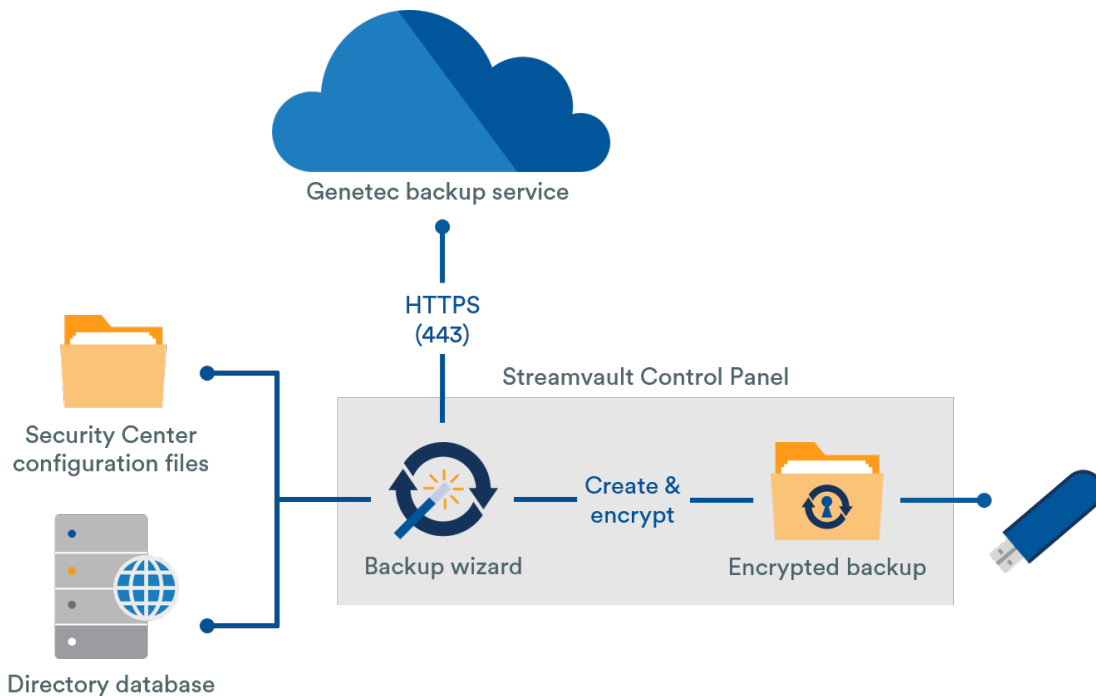
[Habilitación de las características de control de acceso y video de Security Center](#) en la página 27

Acerca de la copia de respaldo y la restauración

Utilizando el Panel de control de SV, puede realizar una copia de seguridad segura de su base de datos del Directorio y de sus archivos de configuración. Más adelante, podrá restaurarlos al mismo ID del sistema en caso de una falla del sistema o una actualización del hardware.

Cómo funciona la copia de seguridad y restauración en el Panel de control de SV

Usted crea copias de seguridad de la base de datos de su Directorio y los archivos de configuración y los almacena en la nube o localmente. En el siguiente diagrama de arquitectura se muestra cómo crear una copia de respaldo de trabajos en SV Control Panel:



Beneficios de la copia de seguridad y la restauración

- Restaure fácilmente cualquiera de las cinco copias de seguridad en la nube o cualquiera de sus copias de seguridad locales al mismo ID del sistema usando el *Restaurar* mago.
- Todos los archivos de copia de respaldo pueden encriptarse.
- El sistema se bloquea después de cinco intentos fallidos de iniciar sesión.
- No necesita inscribirse en el programa Genetec™ Advantage para usar esta característica.

Limitaciones de copia de seguridad y restauración

- Una copia de seguridad excluye sus archivos de licencia, archivos de video u otras bases de datos.
- No puede restaurar una copia de seguridad en una versión anterior de Security Center. Por ejemplo, no puede restaurar una copia de seguridad de un sistema Security Center 5.10 a un sistema Security Center 5.9.
- No puede restaurar los archivos de configuración si la restauración se realiza en versiones superiores de Security Center. Por ejemplo, no puede restaurar los archivos de configuración de una copia de seguridad del sistema Security Center 5.9 a un sistema Security Center 5.10.

Temas relacionados

[Crear una copia de respaldo de la base de datos de su Directory](#) en la página 37

[Restaurar la base de datos de su Directory](#) en la página 38

Crear una copia de respaldo de la base de datos de su Directory

Puede utilizar la copia de seguridad y la restauración para realizar una copia de seguridad segura de su base de datos del Directory y de sus archivos de configuración. La copia de seguridad y la restauración facilitan la configuración de su sistema después de una actualización de hardware y pueden restaurar sus configuraciones después de una falla del sistema.

Antes de empezar

Asegúrese de lo siguiente:

- Se instaló la versión de Security Center 5.9 o una versión posterior.
- Genetec™ Server se está ejecutando.
- Tienes una licencia válida y activa.

Lo que debería saber

- Solo los administradores pueden realizar una copia de seguridad y todas las copias de seguridad en la nube deben estar autenticadas.

Procedimiento

- 1 En el Panel de control de SV, haga clic en el **Configuración** pestaña.
- 2 En *Copia de respaldo/restauración del Directory y las configuraciones*, haga clic en **Asistente de copia de respaldo > Siguiente**.
- 3 Sobre el *Método de copia de seguridad* página, seleccione **Nube** o **Locally** luego haga clic en **Próximo**.
 - Si seleccionó **Nube**, haga lo siguiente:
 - a. En la página de *Autenticación*, introduzca la ID del Sistema o las credenciales del GTAP para autenticar la copia de respaldo.
NOTA: Después de haber introducido sus credenciales por primera vez, no se le volverán a solicitar para realizar futuras copias de seguridad.
 - b. En la página de *Seguridad*, seleccione una de las siguientes dos opciones:
 - **Dejar que Genetec administre mi seguridad:** No es necesario proporcionar una contraseña. El servicio de copia de respaldo en la nube de Genetec Inc. encripta sus datos.
 - **Usar mi propia contraseña:** Cree y recuerde su propia contraseña para usarla más tarde para encriptar sus archivos de respaldo.**IMPORTANTE:** Si pierde u olvida su contraseña, Genetec Inc. no podrá recuperarla.
 - Si seleccionó **Local**, haga lo siguiente:
 - a. En la página de *Carpeta de destino*, introduzca un nombre para la copia de respaldo y navegue hasta la carpeta en la que desea almacenar la copia de respaldo.
 - b. En la página de *Seguridad*, cree una contraseña para encriptar su archivo de respaldo. También puede seleccionar **No encriptar mi copia de seguridad**, aunque no es recomendable.
- 4 Siga el resto de los pasos del asistente para completar su copia de respaldo.

Temas relacionados

[Acerca de la copia de respaldo y la restauración](#) en la página 36

[Restaurar la base de datos de su Directory](#) en la página 38

Restaurar la base de datos de su Directory

Si ha realizado una copia de seguridad de su base de datos del Directory y de sus archivos de configuración usando la copia de seguridad y restauración en el SV Control Panel, puede restaurar sus archivos de copia de seguridad a la misma ID del sistema. Los archivos de la copia de seguridad se pueden restaurar en caso de una falla del sistema o una actualización del hardware.

Antes de empezar

Asegúrese de lo siguiente:

- Se instaló la versión de Security Center 5.9 o una versión posterior.
- Genetec™ Server se está ejecutando.
- Tienes una licencia válida y activa.

Lo que debería saber

- Si creó una copia de respaldo de sus archivos en la nube, puede restaurar cualquiera de las últimas cinco copias de respaldo a la misma ID del Sistema.
- Si realizó una copia de seguridad de sus archivos localmente, puede restaurar cualquiera de sus copias de seguridad al mismo ID del sistema.
- Si creó su propia contraseña para sus archivos de seguridad encriptados durante el proceso de copia de seguridad, la necesitará para restaurar sus archivos.

Procedimiento

- 1 En el Panel de control de SV, haga clic en el **Configuración** pestaña.
- 2 Bajo *Copia de seguridad/Restaurar directorio y configuraciones*, haga clic **Asistente de restauración > Próximo**.
- 3 En la página del *Método de restauración*, seleccione **Nube** o **Local**.
Si seleccionó **Nube**, en la página de *Autenticación*, ingrese su ID del sistema o sus credenciales GTAP, dependiendo de cuál usó para autenticar la copia de seguridad. Si usa las credenciales del GTAP, se le enviará un código de activación a su correo electrónico.
- 4 En la página de *Selección de copia de respaldo*, seleccione el archivo que desea restaurar a su sistema.
- 5 En la página de *Restauración*, si elige crear una contraseña durante el proceso de copia de respaldo, debe introducir su contraseña aquí.
- 6 Siga el resto de los pasos del asistente para completar el proceso de restauración.

Temas relacionados

[Crear una copia de respaldo de la base de datos de su Directory](#) en la página 37

[Acerca de la copia de respaldo y la restauración](#) en la página 36

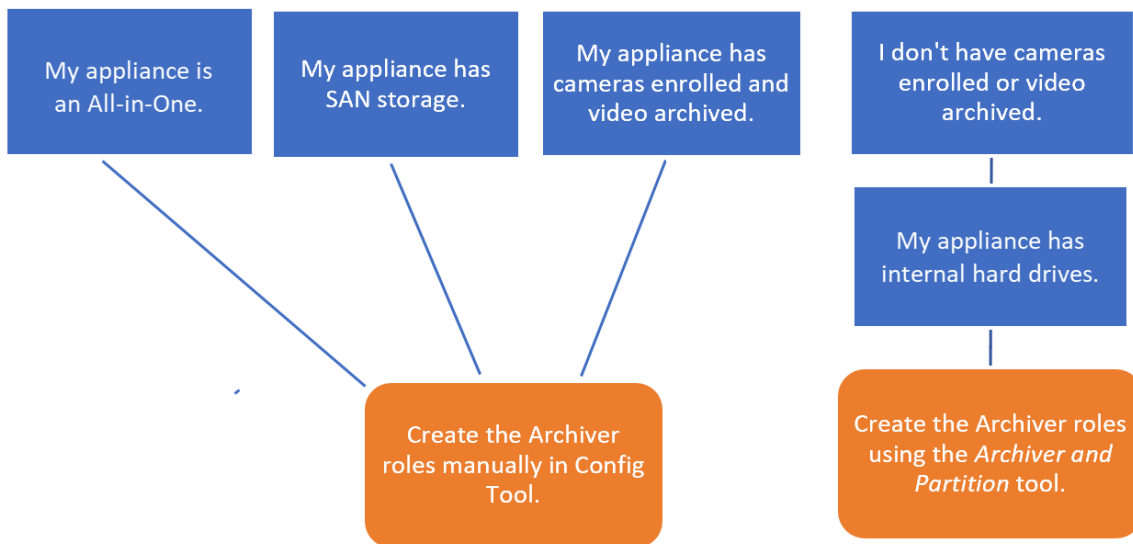
Elegir el método para crear funciones y particiones del Archiver

Para configurar su dispositivo para la cantidad esperada de cámaras y uso de ancho de banda, debe crear suficientes roles de Archiver. Dependiendo del tipo y estado de su electrodoméstico, podrá elegir entre dos métodos.

- [Uso de la herramienta de Funciones y Particiones del Archiver.](#)
- [Crear particiones y funciones de Archiver de forma manual.](#)

Elegir el método para su situación

Utilice el siguiente árbol de decisiones para ayudarle a decidir qué método utilizar:



Acerca de la herramienta de Funciones y Particiones del Archiver

Puede acceder a la herramienta de Funciones y Particiones del Archiver en SV Control Panel. La herramienta calcula cuántas funciones de Archiver necesita según la cantidad de cámaras que planea implementar y su ancho de banda esperado.

Esta herramienta solo está disponible en los modelos Streamvault™ que tienen un disco duro interno. Si está configurando un dispositivo de almacenamiento externo, como SAN en un dispositivo Streamvault™ serie SV-7000EX, siga los pasos que se indican en [Agregar particiones y funciones del Archiver de manera manual](#) en la página 41.

Cuando la herramienta crea particiones, todos los volúmenes locales excepto C: se borran y las funciones de Archiver existentes y las cámaras registradas se eliminan de Security Center. Entonces, si su electrodoméstico tiene cámaras y videos grabados que desea conservar, [agregue manualmente las particiones y los roles de Archiver.](#)

Añadir funciones de Archiver en SV Control Panel

Use la herramienta de Funciones y Particiones del Archiver para agregar suficientes funciones de Archiver para manejar el tráfico de video esperado. Esta herramienta está disponible en dispositivos Archiver de las series Streamvault™ 1000, 2000 y 4000.

Antes de empezar

- Elija el método adecuado para crear funciones y particiones de Archiver.
- Cree una copia de respaldo de los datos importantes en la unidad que quiere particionar.
PRECAUCIÓN: La herramienta Archiver Roles and Partitions puede eliminar datos existentes, incluida la configuración de la función Archiver y todos los archivos en la unidad D:.

Procedimiento

- 1 En el Panel de control de SV, haga clic en el **Configuración** pestaña.
- 2 En *Funciones y particiones del Archiver*, haga clic en **Configurar**.

El *Roles y particiones del archivador* Se abre el cuadro de diálogo.

- 3 Para configurar el número de funciones y particiones del Archiver, seleccione una de las siguientes opciones:
 - Para permitir que la herramienta calcule el número de funciones, el número de particiones y el tamaño de la partición que necesita, seleccione **Escenario sugerido**. Introduzca la cantidad de cámaras que espera implementar y el rendimiento esperado de cada cámara.
 - Para especificar el número de funciones y particiones del Archiver que se crearán, seleccione **Escenario personalizado**. Introduzca el número de funciones del Archiver, el número de particiones y el tamaño de la partición.

La cantidad de particiones debe ser múltiplo de la cantidad de funciones de Archiver.

PRECAUCIÓN: Se eliminan los archivos de la unidad de su partición.

- 4 Hacer clic **Crear particiones y roles..**

Archiver Roles and Partitions

An Archiver role can support:

- 300 cameras
- Throughput of 500 Mbps
- Partitions with a maximum size of 30 TB

Your model (SV-1000-R14-72T-8-210) supports:

- 400 cameras
- 400 Mbps

☒ Suggested scenario

Number of cameras: 0 Number of roles: 0

Camera throughput: 0 Number of partitions: 0

Size of partitions (TB): 0.00

☐ Custom scenario

Number of roles: 0 Total disk space (TB): 0.02

Number of partitions: 0 Used disk space (TB): 0.00

Size of partitions (TB): 0 Free disk space (TB): 0.02

Create partitions/roles

- 5 En la ventana de *Advertencia*, seleccione la casilla de verificación para confirmar que desea continuar.

6 Hacer clic **DE ACUERDO**.

Se abre la ventana de *Resultado* y muestra el nombre y las ubicaciones de las particiones y las funciones del Archiver creadas. A cada función del Archiver se le asigna una letra de unidad de manera automática.

Agregar particiones y funciones del Archiver de manera manual

Para configurar su dispositivo todo en uno Streamvault™ SV-7000EX o SV-300E por primera vez, debe crear las particiones de manera manual. También puede agregar manualmente funciones de Archiver a un dispositivo que ya tenga datos, para que los datos no se pierdan.

Antes de empezar

Elija un método para crear particiones en su dispositivo.

Lo que debería saber

Al formatear un volumen, se eliminan los datos de la partición. Para conservar los datos, reduzca el volumen y luego cree nuevos volúmenes.

Procedimiento

- 1 Si el dispositivo ya tiene cámaras registradas, videos archivados o datos de control de acceso, haga lo siguiente:
 - a) [Realice la copia de respaldo de la base de datos del Directory con SV Control Panel](#).
 - b) Generar un informe de *Configuración de cámaras* para tomar una instantánea de la configuración actual de su cámara. Para obtener información, consulte [Ver la configuración de la cámara](#) en el TechDoc Hub.
- 2 Cree los volúmenes que necesita para las funciones del Archiver que planea crear en el dispositivo.
 - En los dispositivos que se conectan con almacenamiento SAN, como los dispositivos de la serie SV-7000EX, cree un número de unidad lógica (LUN, por sus siglas en inglés) para cada función del Archiver.
 - En los dispositivos que tienen unidades de almacenamiento internas, como SV-1000E, SV-2000E y SV-4000E, utilice la herramienta de *Administración de Discos* de Windows para configurar los volúmenes.

- 3 En Security Center, cree una función de Archiver:
 - a) Desde la página de inicio de Config Tool, abra la tarea de *Sistema* y haga clic en la vista de **Funciones**.
 - b) Haga clic en **Agregar una Entidad** y seleccione **Archiver**.
Se abre el asistente de creación de funciones de Archiver.
 - c) En la página de *información específica*, ingrese un nombre para la **base de datos** de la función del Archiver y haga clic en **Siguiente**.
Cada función de Archiver debe tener una base de datos dedicada.

Creating a role: Archiver

Specific info

Basic information

Creation summary

Entity creation outcome

Database server: (local)\SQLEXPRESS

Database: Archiver5

- d) En el **Información básica** sección, ingrese el **Nombre de la entidad** y haga clic **Próximo**.
Es una buena práctica que el nombre de la base de datos de funciones de Archiver coincida con el nombre de la entidad.

Creating a role: Archiver

Specific info

Basic information

Creation summary

Entity creation outcome

Fill in the following fields. The entity description is optional.

Entity name: Archiver5

Entity description:

- e) Verifique que la información en el *Resumen de creación* la página es correcta y haga clic en **Crear**.
- 4 Configure el rol de archivador.
 - a) En el navegador de entidades, seleccione su nueva función de Archiver y haga clic en **Recursos**.
 - b) Haga clic en **+** para expandir la sección de *Servidor* y seleccione una tarjeta de interfaz de red (NIC, por sus siglas en inglés) de la lista de **Tarjetas de red**.
Todas las funciones de Archiver deben utilizar la misma NIC.


Server: VM9084

Network card: 10.2.110.157 - Ethernet0

RTSP port: 558 and 608

Telnet port: 5605

- c) En *Grabación*, seleccione o cree un **Grupo de discos** o una **Ubicación de Red** para la función de Archiver.
Cada función de Archiver necesita una ubicación de grabación dedicada. Si el Archiver A escribe en los discos A, B y C, entonces el Archiver B debería escribir en los discos D, E y F. Una función puede poseer varias particiones, pero dos funciones nunca deben usar la misma partición.
 - d) Hacer clic **Aplicar**.
- 5 Repita los pasos 3 y 4 para crear cada función del Archiver.

- 6 Agregue sus cámaras a su función del Archiver designada:
 - a) En la página de inicio de Config Tool, abra la tarea de *Video*.
 - b) En el navegador de entidades, seleccione la función del Archiver a la que desea asignar la cámara y haga clic en la **Unidad de video** .
 - c) En el cuadro de diálogo que se abre, ingrese la información requerida sobre la cámara y haga clic en **DE ACUERDO**.

NOTA: Se necesitan unos segundos para agregar las cámaras. Si la función no puede agregar una cámara en el tiempo dado, se indica un estado fallido y se elimina la cámara.
 - d) Hacer clic en **Aplicar**.

Cifrado de la unidad del SO

Para mantener su la seguridad de su dispositivo Streamvault™ y la contraseña de administrador de Windows, debe cifrar la unidad del SO (C:) con BitLocker.

Antes de empezar

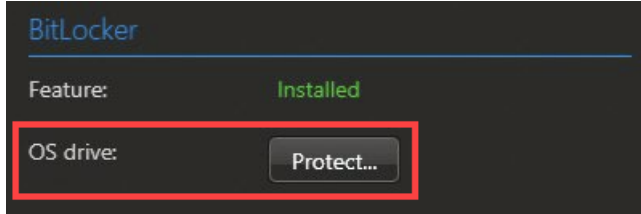
Cuando se cifra la unidad del SO con BitLocker, la clave de cifrado se guarda en un chip de Módulo de Plataforma de Confianza (TPM) ubicada en la placa del sistema del dispositivo Streamvault. Si se retirara la unidad del SO o se reemplazara el tablero del sistema, se perdería la información de la unidad del SO. La unidad del SO no podría tener acceso a la clave de descifrado del TPM. Puede crear una clave de recuperación que puede usarse para descifrar la unidad en estas situaciones. Sin una clave de descifrado, debe volver a crearse una clave del dispositivo y reinstalarse el software.

El disco de almacenamiento se utiliza en primer lugar para almacenar archivos de video y no se cifra con BitLocker. Puede usar las características de Security Center para cifrar archivos de video en períodos de inactividad.

NOTA: La característica de BitLocker está disponible desde SV Control Panel 3.2. La característica también introduce una actualización del perfil de endurecimiento para [dispositivos con capacidades de administración de endurecimiento](#). Puede obtener esta actualización descargando [Servicio Streamvault](#) desde Genetec™ Update Service (GUS) o GTAP. Para aprovechar al máximo la característica de BitLocker, le recomendamos cifrar la unidad del SO y aplicar la actualización del perfil de almacenamiento, si corresponde.

Procedimiento

- 1 En SV Control Panel, haga clic en la pestaña **Seguridad**.
- 2 En la sección *BitLocker*, haga clic en **Proteger** junto al campo **Unidad del SO**.



NOTA: Si la unidad del SO ya está cifrada, en lugar del botón **Proteger** aparece un estado *Protegido*.

- 3 Cuando se le pregunte si desea activar BitLocker, haga clic en **Sí**.
La unidad del SO se cifra, se guarda la clave de cifrado en el TPM y se crea la clave de recuperación. De forma predeterminada, la clave de recuperación se guarda en una unidad de datos fijos. Si no hay una unidad de datos fijos, como en una estación de trabajo, la clave de recuperación se guarda en una memoria USB.
IMPORTANTE: Si guarda la clave de recuperación en una unidad de datos fijos, asegúrese de pasar la clave a una ubicación segura y eliminarla del dispositivo.
- 4 (Opcional) Si no hay una unidad de datos fijos o memoria USB, puede elegir si desea continuar con el cifrado sin crear una clave de recuperación. Realice una de las siguientes acciones:
 - Haga clic en **Sí** para continuar sin crear una clave de recuperación.
 - Haga clic en **No** para cancelar el cifrado.

NOTA: Si elige no crear una clave de recuperación, puede crearla más tarde. Para obtener más información, consulte [Creación de una clave de recuperación](#) en la página 45.

Creación de una clave de recuperación

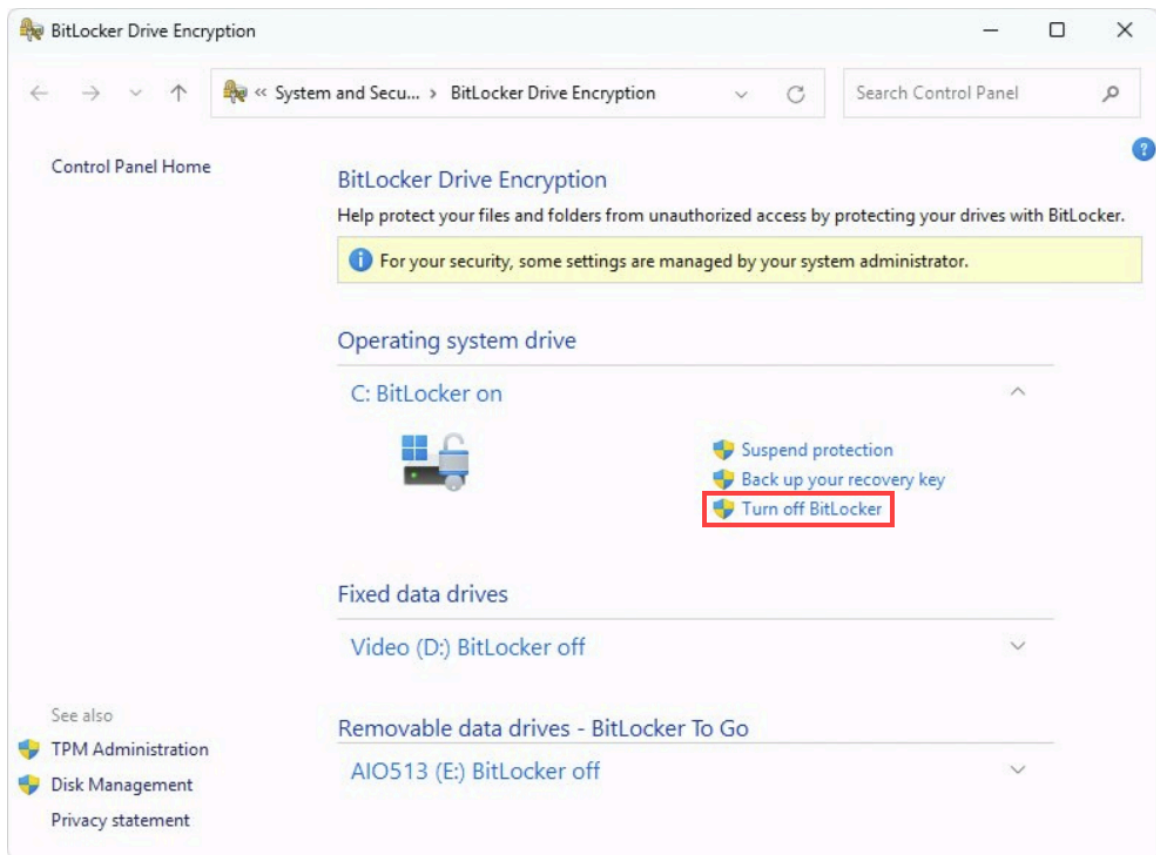
Si ha cifrado la unidad del SO en su dispositivo Streamvault™ con BitLocker pero no ha guardado una clave de recuperación, puede crear una con el cifrado de unidad con BitLocker de Windows.

Lo que debería saber

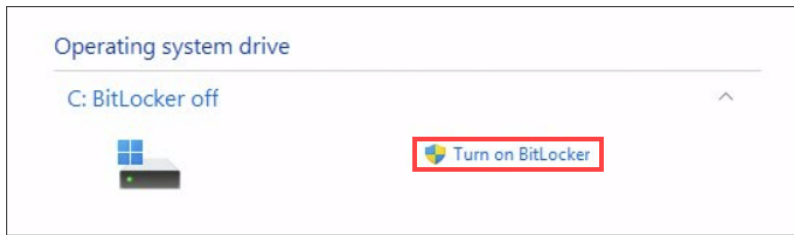
Este procedimiento presupone que ha cifrado la unidad del SO mediante SV Control Panel.

Procedimiento

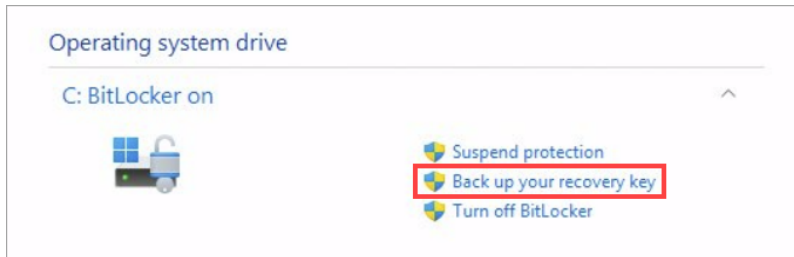
- 1 Desde el menú de inicio de Windows, escriba BitLocker y seleccione **Administrar BitLocker** de los resultados.
Se abre la ventana *Cifrado de unidades con BitLocker*. Se enumeran todas las unidades conectadas al dispositivo.
- 2 En la sección *Unidad del sistema operativo*, haga clic en **Deshabilitar BitLocker** y espere a que se descifre la unidad del SO. Este proceso demora varios minutos.



- 3 Después de descifrar la unidad del SO, haga clic en **Habilitar BitLocker** y espere a que vuelva a cifrarse la unidad del SO con BitLocker.



- 4 Después de cifrar la unidad del SO, haga clic en **Crear copia de respaldo de su clave de recuperación** junto a la unidad del SO (C:).

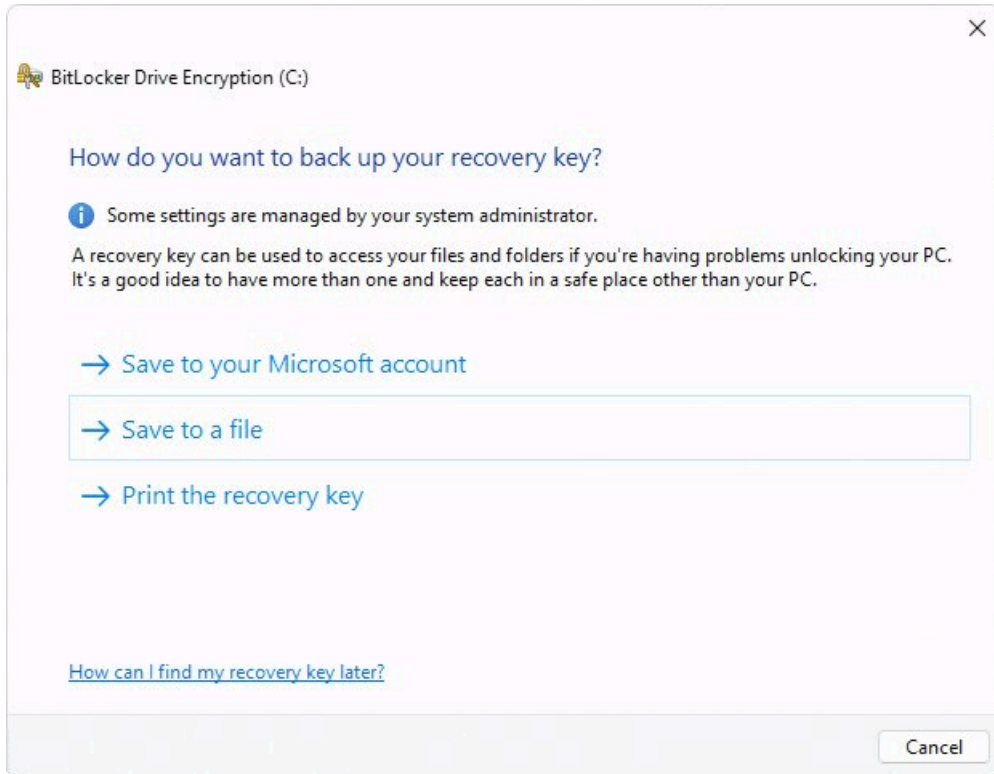


Se abre el asistente de *Cifrado de unidades con BitLocker*.

5 Elija cómo desea crear una copia de seguridad de su clave de recuperación:

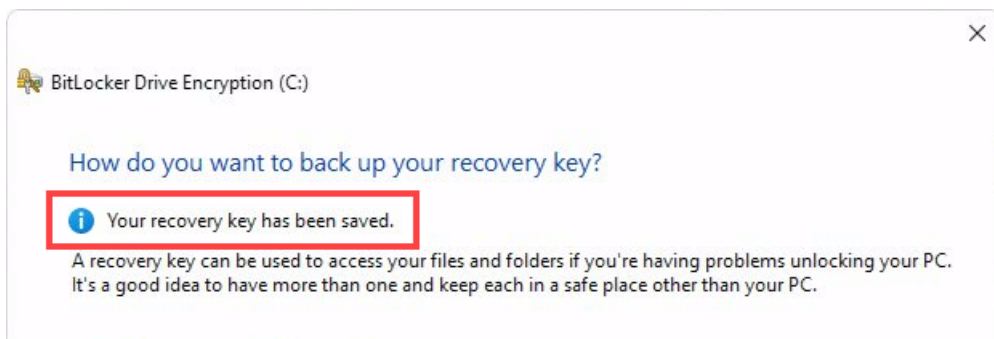
- **Guardar en su cuenta de Microsoft:** Guardar la clave de recuperación en la *biblioteca de claves de recuperación* de su cuenta de Microsoft.
- **Guardar en un archivo:** Guardar su clave de recuperación como archivo de texto sin formato en una unidad de datos fijos sin cifrar en el dispositivo o en una memoria USB.
- **Imprimir la clave de recuperación:** Imprimir una copia física de su clave de recuperación

NOTA: Si selecciona **Guardar a un archivo**, asegúrese de que haya una unidad de datos fijos o memoria USB disponible para guardar la clave de recuperación.



6 Si está guardando la clave de recuperación en un archivo, seleccione la ubicación donde desea guardar la clave y haga clic en **Guardar**.

Se le notificará que se ha guardado la recuperación.



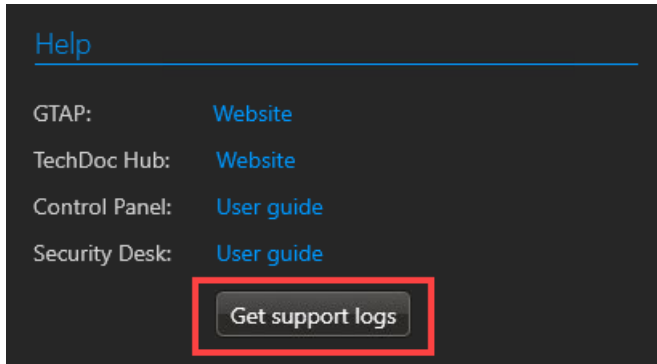
7 Haga clic en **Finalizar** para salir del asistente.

Recopilación de registros de soporte

Genetec™ Technical Assistance Center (GTAC) puede usar sus registros de Streamvault™ y otros registros de aplicación para solucionar problemas de su aplicación. Puede descargar estos registros de soporte desde SV Control Panel.

Procedimiento

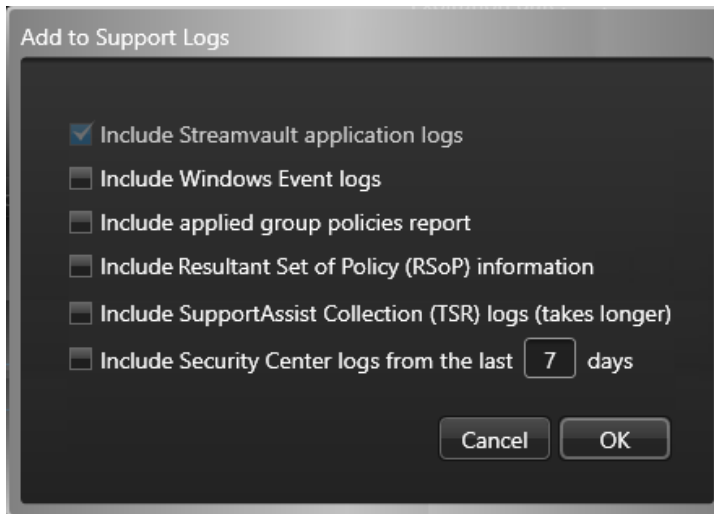
- 1 En SV Control Panel, haga clic en la pestaña **Acerca de**.
- 2 En la sección *Ayuda*, haga clic en **Obtener registros de soporte**.



- 3 En el cuadro de diálogo *Agregar a registros de soporte* que se abre, seleccione los registros que desea descargar.
 - **Registros de aplicaciones de Streamvault:** Estos registros incluyen archivos de registros de Cylance, OEM, políticas, Software y SV Control Panel. Esta opción está seleccionada de forma predeterminada y no puede eliminarse.
 - **Registros de eventos de Windows:** Estos registros incluyen aplicaciones de Windows, seguridad y eventos del sistema.
 - **Informe de políticas de grupo aplicadas:** Este informe es para sistemas que son parte del dominio. El informe enumera todos los objetos de políticas de grupos (GPO) que se hacen cumplir en este momento, y si se aplican a nivel local o de dominio.
 - **Conjunto resultante de información de políticas (RSoP, por sus siglas en inglés):** Este informe de HTML incluye todos los ajustes del sistema configurados a través de políticas de grupo. Para los sistemas no conectados a un dominio, esta opción está seleccionada de forma predeterminada. Para sistemas conectados a un dominio, esta opción está desactivada de forma predeterminada, puesto que el informe contiene información confidencial, como el nombre de dominio, el nombre de host de la aplicación, etc.
 - **Registros de colección de SupportAssist (TSR):** Estos registros son para sistemas que pueden crear una colección de SupportAssist, conocida también como un reporte de soporte técnico (TSR, por sus siglas en inglés). Los servidores de Dell PowerEdge, como servidores Streamvault de las series 1000,

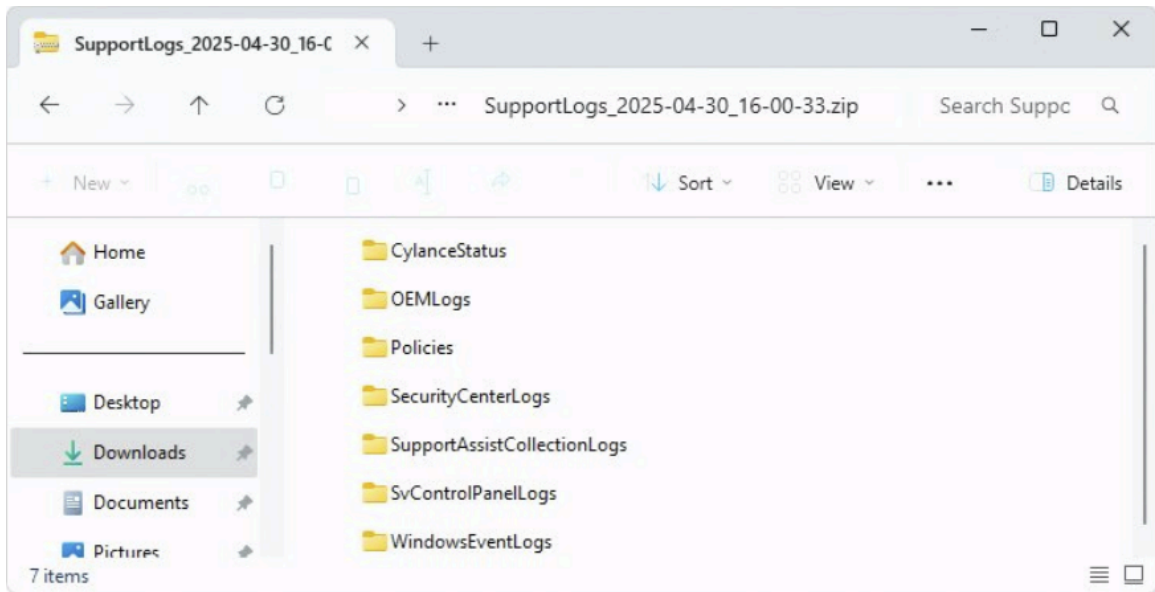
2000, 4000 y 7000, pueden crear colecciones de SupportAssist. Esta opción solo está disponible para los servidores Streamvault que admiten iDRAC.

- **Registros de Security Center de los últimos X días:** De forma predeterminada, se recopilan los registros de Security Center de los últimos 7 días. Introduzca su cantidad preferida de días.



- Haga clic en **Aceptar**.
- En el cuadro de diálogo *Buscar carpeta*, seleccione la carpeta en la que desea guardar sus registros y haga clic en **Aceptar**.

Sus registros de soporte se guardan en una carpeta *.zip*.



Primeros pasos con el plugin Streamvault Maintenance

Comenzar presenta el Streamvault Maintenance complemento y proporciona información sobre cómo configurar el complemento.

Esta sección incluye los temas siguientes:

- ["Acerca de Streamvault Maintenance enchufar"](#) en la página 51
- ["Descargando e instalando el complemento"](#) en la página 52
- ["Privilegios de Genetec Streamvault"](#) en la página 53
- [" Crear la función de plugin "](#) en la página 55
- ["Configuración de una entidad de monitorización de hardware de Streamvault"](#) en la página 56
- ["Configurar una entidad de administrador de Streamvault"](#) en la página 60
- [" Acerca de la pestaña de Administración "](#) en la página 63
- ["Revisar la salud del dispositivo Streamvault"](#) en la página 64
- ["Columnas del panel de informes para la tarea de hardware de Streamvault"](#) en la página 65
- ["Creación de eventos a toma de acción para eventos de estado de Streamvault"](#) en la página 66

Acerca de Streamvault Maintenance enchufar

El plugin de mantenimiento Streamvault™ se usa para monitorear el estado de sus dispositivos Streamvault™ y garantizar que reciba notificaciones cuando se presenten problemas.

NOTA: Esta guía es aplicable al plugin de mantenimiento Streamvault 2.0.

El Streamvault Maintenance El complemento incluye los siguientes componentes:

- **Función Streamvault:** Función de plugin que se utiliza ya sea para ejecutar el monitor de hardware o la entidad Manager. Se requiere una función para cada dispositivo Streamvault que necesite monitorear.
- **Monitor de hardware de Streamvault™:** Entidad que se utiliza para definir las configuraciones de alerta para cada dispositivo Streamvault.
- **Administrador de Streamvault™:** entidad que se utiliza para controlar de forma masiva las configuraciones de un grupo de dispositivos Streamvault. Solo se puede crear una instancia del Streamvault manager.
- **Hardware de Streamvault™:** Tarea de informe en Security Center utilizada para ver una lista de problemas de salud que afectan sus dispositivos Streamvault.

Las configuraciones de la entidad del plugin constan de las siguientes configuraciones:

- **Configuraciones de alerta:** utilizado para definir los tipos de **Eventos**, niveles de **Gravedad** y tipos de **Notificaciones** que afectan las alertas que abordan los estados de salud de sus servidores Streamvault.
- **Destinatarios de correo electrónico:** se utilizan para seleccionar qué usuarios y grupos de usuarios reciben notificaciones por correo electrónico.
- **Credenciales de administración remota:** se utilizan para controlar la creación de perfiles de usuario en iDRAC.
- **Integración integrada de Dell Remote Access Controller (iDRAC)** (para modelos de Streamvault que admiten iDRAC): se utiliza para ejercer un control más preciso en la administración de credenciales. Esta característica se puede encontrar en la pestaña de **Administración** del plugin.

Para obtener más información sobre iDRAC, consulte <https://www.dell.com/en-us/lp/dt/open-manage-idrac>.

IMPORTANTE:

- Para sistemas con servidores habilitados para iDRAC, el firmware de iDRAC debe tener la versión 6.0 o una versión posterior.
- Para los dispositivos compatibles con iDRAC, el plugin Streamvault Maintenance accede a los datos del estado de salud mediante una conexión interna, siempre que el software del módulo de servicio iDRAC (ISM) de Dell esté instalado. ISM se instala de forma predeterminada en los modelos compatibles con iDRAC.

Si ISM no está disponible, el plugin utiliza la comunicación fuera de banda con iDRAC. En este caso, debe existir una conexión de red entre el puerto exclusivo de iDRAC y al menos un puerto LAN si no se comparte el puerto. El puerto iDRAC dedicado está deshabilitado de forma predeterminada. Para obtener más información, consulte lo siguiente: <https://www.dell.com/support/kbdoc/en-ca/000177212/dell-poweredge-how-to-configure-the-idrac9-and-the-lifecycle-controller-network-ip>.

Descargando e instalando el complemento

Para integrar el plugin Streamvault™ Maintenance en Security Center, debe instalar el plugin en un servidor del Directory, los servidores de Streamvault™ que desee monitorear y en todas las estaciones de trabajo cliente desde las que desee configurar el plugin.

Antes de empezar

Asegúrese de que esté instalada una versión compatible de Security Center. Para obtener más información, consulte los [Plugins compatibles con Security Center](#) en el TechDoc Hub.

Lo que debería saber

- **MEJOR PRÁCTICA:** Instale la función Streamvault en cada servidor que necesite monitorear.
- **IMPORTANTE:** Asegúrese de que el módulo iDRAC de cada servidor esté conectado a su red y pueda comunicarse con el sistema host. De manera predeterminada, el módulo iDRAC comparte el mismo puerto LAN que el sistema host y está configurado para obtener una dirección IP mediante DHCP.
- **IMPORTANTE:** Antes de continuar, asegúrese de que el módulo iDRAC esté actualizado al firmware 6.00 o una versión posterior y que el BIOS del servidor esté actualizado a la última versión.
- El plugin solo es compatible con servidores que ejecuten el software del servidor de Security Center.
- **NOTA:** El [Streamvault Maintenance enchufar](#) viene preinstalado en todos los servidores Streamvault compatibles. Por eso, la mayoría de los usuarios solo necesita crear las funciones y las entidades en Security Center. Si su servidor se envió antes de que el complemento estuviera disponible, o si se desinstaló, siga estos pasos para instalarlo.

Procedimiento

- 1 Abre el GTAP [Descarga del producto](#) página.
- 2 En la sección de **Buscador de Descargas**, seleccione su versión de Security Center.
- 3 Desde la sección de *Plugins de Genetec*, descargue el paquete de su producto.
- 4 Ejecute el archivo .exe y, luego, descomprímalo.
De manera predeterminada, el archivo se descomprime en C:\Genetec.
- 5 Abra la carpeta extraída, haga clic con el botón derecho en el archivo *setup.exe* y, luego, haga clic en **Ejecutar como administrador**.
- 6 Siga las instrucciones de instalación.
- 7 En la página de *Asistente de Instalación Completado*, haga clic en **Finalizar**.
IMPORTANTE: El **Reinicie el servidor Genetec™** La opción está seleccionada de forma predeterminada. Puede desmarcar esta opción si no desea reiniciar el Genetec™ Server de inmediato. Sin embargo, debe reiniciar Genetec Server para completar la instalación.
- 8 Cierre y luego abra cualquier instancia de Config Tool y Security Desk.

Privilegios de Genetec Streamvault

Para utilizar las tareas de *Monitor de hardware* y *Administrador* asociadas con el dispositivo Streamvault™, las cuentas de usuario deben tener asignados los privilegios necesarios.

Configurar privilegios de usuario para Streamvault

Los privilegios predeterminados se asignan a algunos grupos de usuarios, como los administradores.

En la herramienta de configuración *Gestión de usuarios* tarea, puede configurar o modificar los privilegios de usuario o grupo de usuarios en la *Privilegios* página del usuario o grupo de usuarios.

Para obtener más información sobre la jerarquía de privilegios, la herencia de privilegios y la asignación de privilegios, consulte la [Guía del Administrador de Security Center](#) y la [Guía de Endurecimiento de Security Center](#) en el TechDoc Hub.

NOTA: Para obtener una lista de todos los privilegios disponibles de Security Center, consulte la [Privilegios del Centro de seguridad](#) hoja de cálculo. Puede ordenar y filtrar esta lista según lo necesite.

Privilegios de la función del plugin Streamvault

Los privilegios de la función del plugin Streamvault otorgan acceso a las tareas asociadas con Streamvault *Monitor de hardware* y *Administrador*.

De forma predeterminada, los administradores tienen todos los privilegios. Si crea una cuenta de usuario a partir de una de las otras plantillas de privilegios, la cuenta de usuario requiere los siguientes privilegios de la función del plugin Streamvault para Config Tool en Streamvault.

Subcategoría de privilegios	Incluye privilegios para	Acciones que se pueden realizar
Monitor de hardware	Modificar monitores de hardware	<ul style="list-style-type: none"> • Modificar configuraciones de alerta • Modificar destinatarios de correo electrónico • Modificar las credenciales de administración remota • Cambiar la configuración del puerto
	Agregar monitores de hardware	Crear una nueva entidad de monitor de hardware y asignársela a un servidor de Streamvault
	Eliminar monitores de hardware	Eliminar una entidad de monitor de hardware existente
	Ver monitores de hardware	Ver una configuración de monitor de hardware
Administrador	Modificar administrador	<ul style="list-style-type: none"> • Modificar configuraciones de alertas de manera masiva • Modificar destinatarios de correo electrónico de manera masiva

Subcategoría de privilegios	Incluye privilegios para	Acciones que se pueden realizar
	Agregar administrador	Crear la entidad administradora y asignarla a un servidor de Streamvault
	Borrar administrador	Eliminar la entidad administradora
	Ver administrador	Ver la configuración del administrador

Crear la función de plugin

Antes de poder configurar y utilizar el complemento, debe crear la función del complemento de mantenimiento Streamvault™ en Config Tool.

Antes de empezar

[Descargue e instale el complemento.](#)

Lo que debería saber

El Streamvault Maintenance El complemento contiene dos funciones de complemento:

- **Monitor de hardware Streamvault™:** La entidad de monitor de Hardware de Streamvault™ se usa para monitorear el estado de sus dispositivos Streamvault™ y garantizar que reciba notificaciones cuando ocurran problemas. Se requiere un monitor de hardware Streamvault™ por dispositivo Streamvault™.
- **Streamvault™ manager:** La entidad Streamvault™ Manager se usa para controlar las configuraciones de alertas para un grupo de entidades de Streamvault™ Agent. Solo se permite un administrador Streamvault™ por sistema.
- **NOTA:** Si los servidores del Directory son máquinas virtuales o servidores que no son de Streamvault, cree una función para estos servidores solo si desea utilizar la entidad Manager.

Procedimiento

- 1 Desde la página de inicio de Config Tool, abra el *Complementos* tarea.
- 2 En la tarea de *Plugins*, haga clic en **Agregar una entidad** (+) y seleccione **Plugin**.
Se abre el asistente de creación de plugins.
- 3 Sobre el *información específica* página, seleccione el servidor en el que está alojada la función del complemento y el tipo de complemento, y luego haga clic en **Próximo**.
Si no utiliza servidores de expansión en su sistema, no se muestra la opción de **Servidor**.
- 4 Sobre el *Información básica* página, especifique la información del rol:
 - a) Introduzca el **Nombre de la entidad**.
 - b) Introduzca la **Descripción de la entidad**.
 - c) Seleccione el **Dividir** para la función del complemento.
Si no utiliza particiones en su sistema, no se muestra la opción de **Partición**. Las particiones son agrupaciones lógicas que se utilizan para controlar la visibilidad de las entidades. Solo los usuarios que son miembros de esa partición pueden ver o modificar la función.
 - d) Haga clic en **Siguiente**.
- 5 En la página *Resumen de creación*, revise la información y luego haga clic en **Crear** o **Atrás** para hacer cambios.
Después de crear la función del plugin, aparece el siguiente mensaje: La operación fue exitosa.
- 6 Haga clic en **Cerrar**.

Después de que concluya

- [Configurar la entidad de monitoreo de hardware de Streamvault.](#)
- [Configurar la entidad de Streamvault manager.](#)

Configuración de una entidad de monitorización de hardware de Streamvault

Puede configurar una entidad de monitor de hardware de Streamvault™ para monitorear la salud de un dispositivo Streamvault™ y configurar las notificaciones para que se generen cuando ocurran problemas.

Antes de empezar

- Inscriba sus dispositivos Streamvault.
- [Crear la función de plugin Streamvault.](#)

IMPORTANTE: Se crea un monitor de hardware Streamvault de manera automática en cada servidor de Streamvault que aloje una función de Streamvault. Si la entidad de monitor de hardware no está presente en su sistema después de haber creado la función, debe crear el monitor de hardware de manera manual. El monitor de hardware solo puede ejecutarse en un servidor de Streamvault.

Lo que debería saber

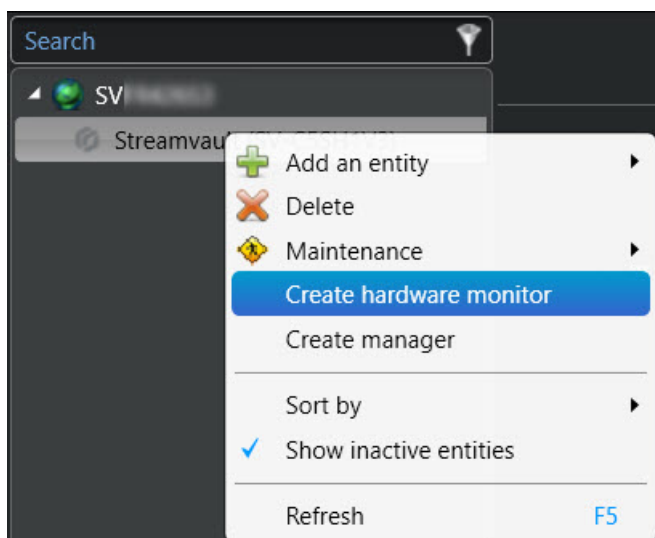
Las opciones de configuración son diferentes dependiendo de si tiene servidores habilitados para iDRAC u otros servidores que no son iDRAC.

- [Configuración de un servidor habilitado para iDRAC.](#)
- [Configuración de un servidor que no sea iDRAC.](#)

Procedimiento

Para configurar un servidor habilitado para iDRAC:

- 1 En Config Tool, navegue hasta el *Complementos* tarea y seleccione la función del complemento Streamvault.
- 2 Haga clic derecho en la función de plugin Streamvault y haga clic en **Crear monitor de hardware**.



- 3 Desde la pestaña de **Identidad**, introduzca un nombre para el monitor de hardware de Streamvault en el campo de **Nombre**.
- 4 Seleccione la pestaña de **General**.

- 5 (Opcional) Si creó una entidad de Streamvault™ manager para su sistema, seleccione la casilla de verificación de **Usar la configuración del administrador** para usar los ajustes del perfil de configuración de alertas del Streamvault manager.
- 6 En la sección de *Perfil de configuración de alertas*, seleccione la casilla de verificación **El monitor de hardware administra las configuraciones de alertas de iDRAC** para administrar las configuraciones de alerta a través del monitor de hardware Streamvault.
- 7 Seleccione las casillas de verificación que se correlacionan con los **Eventos**, los niveles de **Gravedad** y los tipos de **Notificaciones** que desea incluir para este monitor de hardware Streamvault.

Events	Severity			Notification	
	Critical	Warning	Information	Email	Event
Cooling	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
CPU	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Memory	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Networking	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Power	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Storage	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
System	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

- 8 En la sección de *Destinatarios del correo electrónico*, elija qué usuarios y grupos de usuarios recibirán notificaciones por correo electrónico cuando se cumpla una condición en la sección de *Perfil de configuración de alertas*.

Recipient	Selected
Admin	<input type="checkbox"/>
Administrators	<input checked="" type="checkbox"/>
AutoVu	<input type="checkbox"/>
AutoVu operators	<input type="checkbox"/>
Patroller	<input type="checkbox"/>
Patroller users	<input type="checkbox"/>

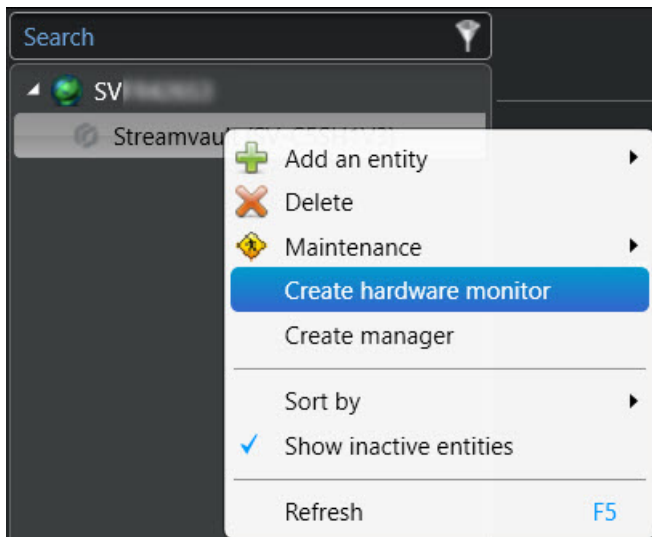
- 9 En la sección de *Credenciales de administración remota*, realice una de las siguientes acciones:
 - Seleccione la casilla de verificación **El monitor de hardware administra las cuentas de iDRAC** para administrar las credenciales de manera directa a través del plugin.
 - Limpie la casilla de verificación **El monitor de hardware administra las cuentas de iDRAC** para usar iDRAC para controlar la creación de usuarios y contraseñas.
- 10 (Opcional) Si borró la casilla de verificación de **El monitor de hardware administra las cuentas de iDRAC**, vaya a la pestaña de **Administración** y configure las credenciales de manera directa en iDRAC.

- 11 (Opcional) En la sección de *Ajustes*, puede cambiar el valor predeterminado **Puerto entrante** desde 65115 hasta su opción favorita. Para más información, ver [Puertos predeterminados utilizados por Streamvault](#) en la página 4.

- 12 Haga clic en **Aplicar**.

Para configurar un servidor que no sea iDRAC:

- 1 En Config Tool, navegue hasta el *Complementos* tarea y seleccione la función del complemento Streamvault.
- 2 Haga clic derecho en la función de plugin Streamvault y haga clic en **Crear monitor de hardware**.



- 3 Desde la pestaña de **Identidad**, introduzca un nombre para el monitor de hardware de Streamvault en el campo de **Nombre**.
- 4 Seleccione la pestaña de **General**.
- 5 (Opcional) Si creó una entidad de Streamvault manager para su sistema, seleccione la casilla de verificación de **Usar la configuración del administrador** para usar los ajustes del perfil de configuración de alertas del Streamvault manager.
- 6 En la sección de *Perfil de configuración de alertas*, seleccione las casillas de verificación que se correlacionan con los **Eventos** y los tipos de **Notificaciones** que desea aplicar a las Streamvault Maintenance instancias del plugin controladas por Streamvault manager.
- 7 En **Configuración**, establezca el **% del umbral** de desgaste de la unidad de estado sólido (SSD) en la que desea recibir una notificación para informarle que debe reemplazar la SSD pronto.

- 8 En la sección de *Destinatarios del correo electrónico*, elija qué usuarios y grupos de usuarios recibirán notificaciones por correo electrónico cuando se cumpla una condición en la sección de *Perfil de configuración de alertas*.

☐ Use manager settings

Alert configuration profile

Events	Notification	Event	Status	Configuration
	Email	Event		
Predictive drive failure	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> Normal	Threshold % <input type="text" value="90"/>
SSD wear	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> Normal	
Offline drive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		

Email recipients

☐ Admin

☒ Administrators

No email configured for this group

☐ AutoVu

☐ AutoVu operators

☐ Patroller

☐ Patroller users

- 9 Hacer clic **Aplicar**.

Temas relacionados

[Acerca de la pestaña de Administración](#) en la página 63

Configurar una entidad de administrador de Streamvault

Puede configurar una entidad de Streamvault™ manager para controlar las configuraciones de alertas de un grupo de monitores de hardware de Streamvault™ desde una sola ubicación. También puede configurar las notificaciones para que se generen cuando ocurran problemas. El uso de la entidad Streamvault manager es opcional.

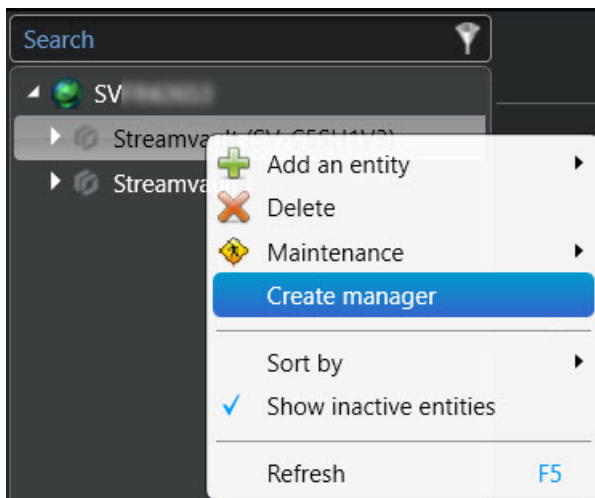
Antes de empezar

- Inscriba sus dispositivos Streamvault™.
- [Crear la función de plugin Streamvault.](#)

NOTA: La entidad Streamvault manager puede ejecutarse en cualquier servidor (Streamvault o no Streamvault) o máquina virtual (VM, por sus siglas en inglés) en su sistema de Security Center. Solo se puede agregar una entidad de Streamvault manager al sistema.

Procedimiento

- 1 En Config Tool, navegue hasta el *Complementos* tarea y seleccione la función del complemento Streamvault.
- 2 Haga clic derecho en la función de plugin de Streamvault y haga clic en **Crear administrador**.



- 3 Seleccione la entidad del Streamvault manager y haga clic en la pestaña de **General**.

Se muestran las siguientes secciones:

- La sección del *Perfil de configuración de alertas de iDRAC* administra los servidores habilitados para iDRAC en su sistema.
- La sección de *Perfil de configuración de alertas que no son de iDRAC* se usa para administrar otros servidores que no son iDRAC en el sistema.

Ambas secciones siempre se muestran, ya sea que tengan un sistema iDRAC o no.

- 4 (Si corresponde) En la sección de *Perfil de configuración de alertas de iDRAC*, configure lo siguiente:
- Para administrar las configuraciones de alerta de iDRAC a través del monitor de hardware Streamvault del servidor seleccionado, seleccione la casilla de verificación de **El monitor de hardware administra las configuraciones de alertas de iDRAC**.
 - Seleccione las casillas de verificación que se correlacionan con los **Eventos**, los niveles de **Gravedad** y los tipos de **Notificaciones** que desea aplicar a las Streamvault Maintenance instancias del plugin controladas por Streamvault manager.

Events	Severity			Notification	
	Critical	Warning	Information	Email	Event
Cooling	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
CPU	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Memory	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Networking	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Power	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Storage	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
System	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Hardware monitors using Streamvault™ manager configuration

Streamvault (SV-C5SH1V3) - Streamvault™ hardware monitor

NOTA: Los monitores de hardware cuyas configuraciones están establecidas por el Streamvault manager se enumeran en **Monitores de hardware que utilizan la configuración del Streamvault™ manager**. Los monitores de hardware que usan sus propias configuraciones se enumeran en **Monitores de hardware que usan una configuración personalizada**.

- 5 (Si corresponde) En la sección de *Perfil de configuración de alertas que no son de iDRAC*, configure lo siguiente:
 - a) Seleccione las casillas de verificación que se correlacionan con los **Eventos** y los tipos de **Notificaciones** que desea aplicar a las Streamvault Maintenance instancias del plugin controladas por Streamvault manager.
 - b) En **Configuración**, establezca el **% del umbral** de desgaste de la unidad de estado sólido (SSD) en la que desea recibir una notificación para informarle que debe reemplazar la SSD pronto.

Events	Notification		Configuration
	Email	Event	
Predictive drive failure	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Threshold % <input type="text" value="90"/>
SSD wear	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Offline drive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	

Hardware monitors using Streamvault™ manager configuration

Streamvault (SVFR426S3) - Streamvault™ hardware monitor

NOTA: Los monitores de hardware cuyas configuraciones están establecidas por el Streamvault manager se enumeran en **Monitores de hardware que utilizan la configuración del Streamvault™ manager**. Los monitores de hardware que usan sus propias configuraciones se enumeran en **Monitores de hardware que usan una configuración personalizada**.

- 6 En la sección de *Destinatarios del correo electrónico*, elija qué usuarios y grupos de usuarios recibirán notificaciones por correo electrónico cuando se cumpla una condición en la sección de **Perfil de configuración de alertas de iDRAC** o **Perfil de configuración de alertas que no son de iDRAC**.

Email recipients

- ☐ Admin
- ☒ Administrators No email configured for this group
- ☐ AutoVu
- ☐ AutoVu operators
- ☐ Patroller
- ☐ Patroller users

- 7 Hacer clic **Aplicar**.

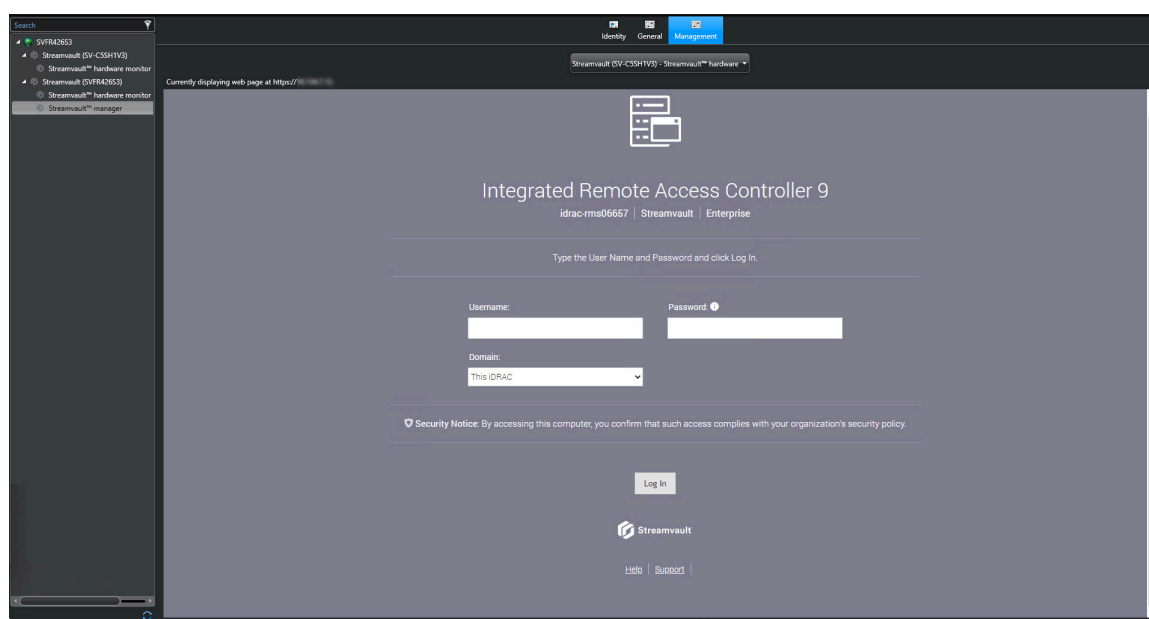
Acerca de la pestaña de Administración

La pestaña de **Administración** muestra una página web de iDRAC con la que puede configurar y administrar las credenciales del servidor de iDRAC. También puede encontrar más información sobre su servidor iDRAC y configurar otras opciones que no están disponibles a través de la interfaz de usuario del plugin de Streamvault™.

Puede acceder a la pestaña de **Administración** a través del monitor de hardware Streamvault™ de cualquier servidor habilitado para iDRAC o a través del administrador de Streamvault™.

Si accede a la pestaña de **Administración** a través del administrador de Streamvault, verá un menú desplegable en la parte superior de la página. Puede usarlo para cambiar de un servidor iDRAC a otro en lugar de tener que cambiar de manera manual de un monitor de hardware a otro. Cada servidor de iDRAC tiene su propia página web de iDRAC.

Para obtener información de inicio de sesión, haga clic en **Ayuda** en la parte inferior de la página web.



NOTA: Para acceder a la página web de iDRAC, necesita una conexión de red entre el sistema cliente que ejecuta Config Tool y la dirección IP del servidor de iDRAC. Si una conexión de red no está disponible, use la página de Config Tool de manera directa desde el dispositivo de Streamvault a través de un escritorio remoto o una sesión de consola local.

Si su sistema no tiene servidores de iDRAC, la pestaña de **Administración** está vacía. Un mensaje indica que no hay monitores de hardware Streamvault con capacidades de administración de iDRAC disponibles.

NOTA: Si la página web de iDRAC no carga, haga clic en otra pestaña y luego regrese a la pestaña de **Administración**.

Temas relacionados

[Configuración de una entidad de monitorización de hardware de Streamvault](#) en la página 56

[Configurar una entidad de administrador de Streamvault](#) en la página 60

Revisar la salud del dispositivo Streamvault

Use la tarea de Hardware de Streamvault™ para ver una lista de problemas de salud que afecten a sus dispositivos Streamvault.

Procedimiento

- 1 Desde la página de inicio, abra la tarea de *Hardware de Streamvault*.
- 2 En el **Intervalo de tiempo** filtro de consulta, defina el período de tiempo que desea que incluya el informe.
- 3 Haga clic en **Generar informe**.
Las propiedades de la unidad se enumeran en el panel del informes.

Columnas del panel de informes para la tarea de hardware de Streamvault

Después de generar un informe, los resultados de su consulta se enumeran en el panel de informes. Esta sección enumera las columnas disponibles para la tarea de hardware de Streamvault™.

- **Imagen:** Ícono que representa el tipo de problema.
- **Gravedad:** Nivel de gravedad asociado con el problema.
- **Marca de tiempo:** Fecha y hora en que ocurrió el problema.
- **Fuente:** Dispositivo Streamvault afectado por el problema.
- **Id. de mensaje:** Secuencia alfanumérica de identificación asociada con el problema que se informó.
- **Mensaje:** Descripción del problema.
- **Descripción:** Descripción de la causa del problema.

NOTA: Para obtener más información sobre la creación de informes, consulte [Descripción general del espacio de trabajo de la tarea de informes](#) en el TechDoc Hub.


Creación de eventos a toma de acción para eventos de estado de Streamvault

Al utilizar un evento a toma de acción, puede activar acciones que ocurrirán cuando se detecte un problema de hardware de Streamvault™.

Antes de empezar

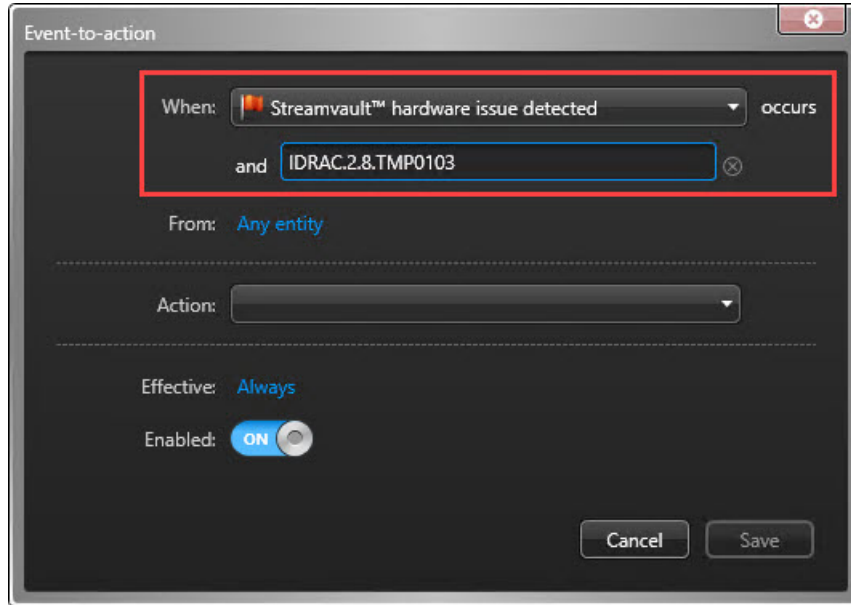
- [Crear la función del plugin de mantenimiento de Streamvault.](#)
- [Configurar una entidad de monitoreo de hardware de Streamvault.](#)

Procedimiento

- 1 Desde la página de inicio de Config Tool, haga clic en la tarea de *Automatización* y luego haga clic en la vista de **Acciones**.
- 2 Haga clic en **Agregar un elemento** .

3 Configure su evento a toma de acción:

- a) Desde el menú desplegable **Cuando**, seleccione **Se detectó un problema de hardware de Streamvault**.
- b) Haga clic en **Especificar una condición** e ingrese el código de error de iDRAC. También puede ingresar la ID completa para evitar activaciones falsas.
Por ejemplo, en la captura de pantalla siguiente, el código de error es TMP0103 y la ID completa es IDRAC.2.8.TMP0103.



- c) (Opcional) En la opción de **Desde**, seleccione su plugin o monitor de hardware de Streamvault™.
NOTA: Dado que el plugin de Streamvault utiliza eventos personalizados que solo tienen significado para él mismo, no es necesario asignar una fuente.
Si selecciona el plugin de Streamvault como entidad de origen, si alguna vez se elimina la función de complemento, se eliminarán todas las reglas de automatización vinculadas. Si no se especifica ninguna entidad de origen y se elimina la función, las reglas de automatización persisten.
- d) Desde el menú desplegable de **Acción**, seleccione un tipo de acción y configure sus parámetros.
- e) (Opcional) En la opción de **Vigencia**, haga clic en **Siempre** y seleccione un horario para cuando este evento a toma de acción esté activo.
Si el evento ocurre fuera del horario definido, entonces la acción no se activa.

4 Asegúrese de que el evento a toma de acción esté habilitado.

5 Hacer clic **Ahorrar**.

NOTA: Para obtener una lista completa de los códigos de error de iDRAC, consulte <https://developer.dell.com/apis/2978/versions/5.xx/docs/Error%20Codes/EEMRegistry.md>.

Referencia de SV Control Panel

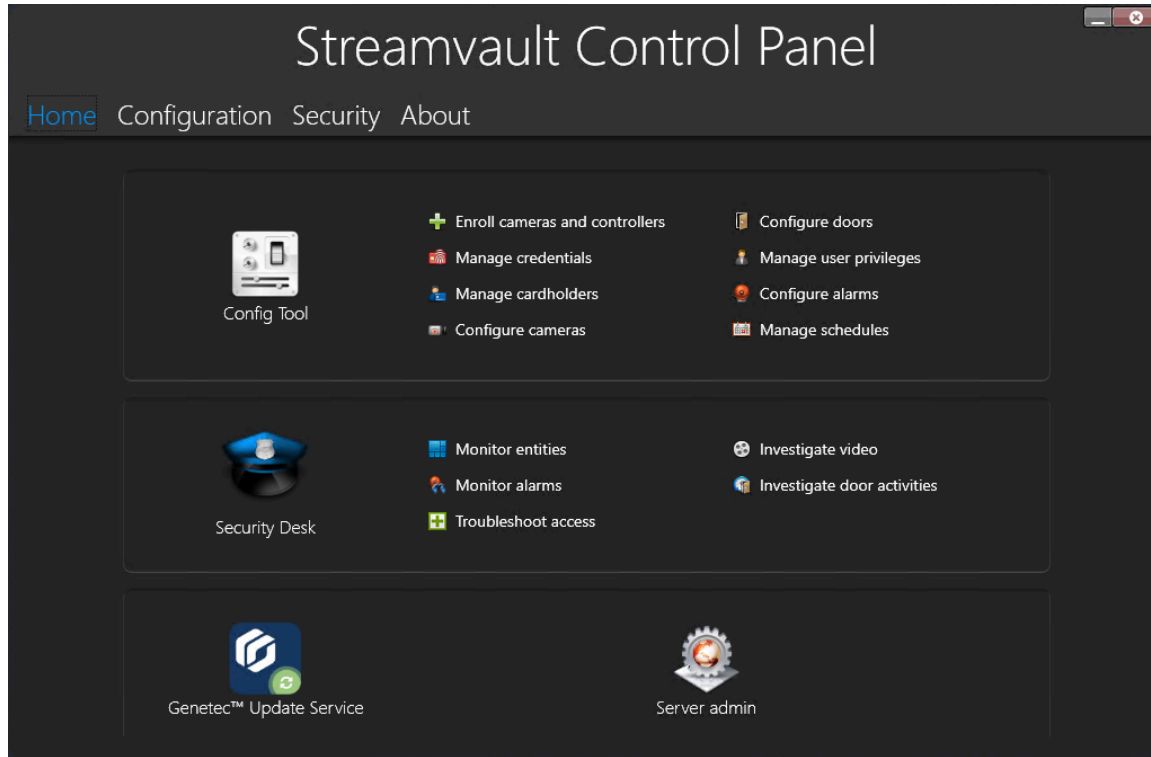
Estas páginas de referencia le ayudarán a comprender el Panel de control de SV.

Esta sección incluye los temas siguientes:

- ["Página de inicio de SV Control Panel"](#) en la página 69
- ["Página de configuración del Panel de Control SV"](#) en la página 71
- ["Página de seguridad del SV Control Panel"](#) en la página 74
- ["Acerca de la página de SV Control Panel"](#) en la página 78

Página de inicio de SV Control Panel

Use la página de inicio de SV Control Panel para acceder a las tareas básicas necesarias para configurar y usar su sistema. Puede hacer clic en los íconos de la interfaz para acceder a las aplicaciones Config Tool, Security Desk, Server Admin o Genetec™ Update Service.



Alternativamente, puede hacer clic en los accesos directos de la herramienta de configuración o en los accesos directos de Security Desk para abrir las tareas asociadas.

Para los sistemas que se ejecutan en modo Cliente, el acceso directo de Server Admin no está disponible. De la misma manera, Config Tool y los accesos directos de Security Desk son limitados.

NOTA: Nota: Si su sistema no está activado, aparecerá un banner rojo para notificarle. Haga clic en **El sistema no está activado. Haga clic aquí para activarlo.** para abrir el asistente de activación del Panel de Control de Streamvault™.

Accesos directos de Config Tool

Utilice los accesos directos para abrir las tareas principales en la aplicación Config Tool. Los accesos directos disponibles dependen de las opciones de licencia que tenga.

Atajo	Acción
Config Tool	Abre Config Tool.
Inscribir cámaras y controladores	Abre la Herramienta de Inscripción de la Unidad, donde puede inscribir sus cámaras y controladores.
Administrar credenciales	Abre la tarea de <i>Administración de credenciales</i> , donde puede administrar las credenciales de usuario.

Atajo	Acción
Administrar tarjetahabientes	Abre la tarea de <i>Administración de tarjetahabientes</i> , donde podrá administrar a los tarjetahabientes.
Configurar cámaras	Abre la tarea de <i>Video</i> , donde podrá agregar y administrar las cámaras.
Configurar puertas	Abre la tarea de <i>Vista del área</i> , donde podrá agregar y administrar las puertas.
Administrar privilegios de usuario	Abre la tarea de <i>Administración de usuarios</i> , donde puede agregar y administrar los privilegios de usuario.
Configurar alarmas	Abre la tarea de <i>Alarmas</i> , donde podrá configurar las alarmas.
Administrar horarios	Abre la tarea de <i>Sistema</i> , donde podrá crear y administrar los horarios.

Accesos directos de Security Desk

Utilice los accesos directos para abrir las tareas principales en la aplicación Security Desk. Los accesos directos disponibles dependen de las opciones de licencia que tenga.

Atajo	Acción
Security Desk	Abre Security Desk.
Supervisar entidades	Abre la tarea de <i>Monitorear</i> , donde puede monitorear los eventos del sistema en tiempo real.
Monitorear alarmas	Abre la tarea de <i>Monitoreo de alarmas</i> , donde puede monitorear y responder a las alarmas activas y ver las alarmas pasadas.
Acceso a la resolución de problemas	Abre la herramienta del Solucionador de problemas de acceso, que le permite diagnosticar y acceder a los problemas de configuración. NOTA: Este acceso directo no está disponible para los sistemas que se ejecutan en modo Cliente.
Investigar video	Abre la tarea de <i>Archivos</i> , donde podrá buscar archivos de video. NOTA: Este acceso directo no está disponible para los sistemas que se ejecutan en modo Cliente.
Investigar actividades de las puertas	Abre la tarea de <i>Actividades de las puertas</i> , donde puede investigar eventos que ocurrieron en puertas seleccionadas. NOTA: Este acceso directo no está disponible para los sistemas que se ejecutan en modo Cliente.

Acceso directo a Genetec Update Service

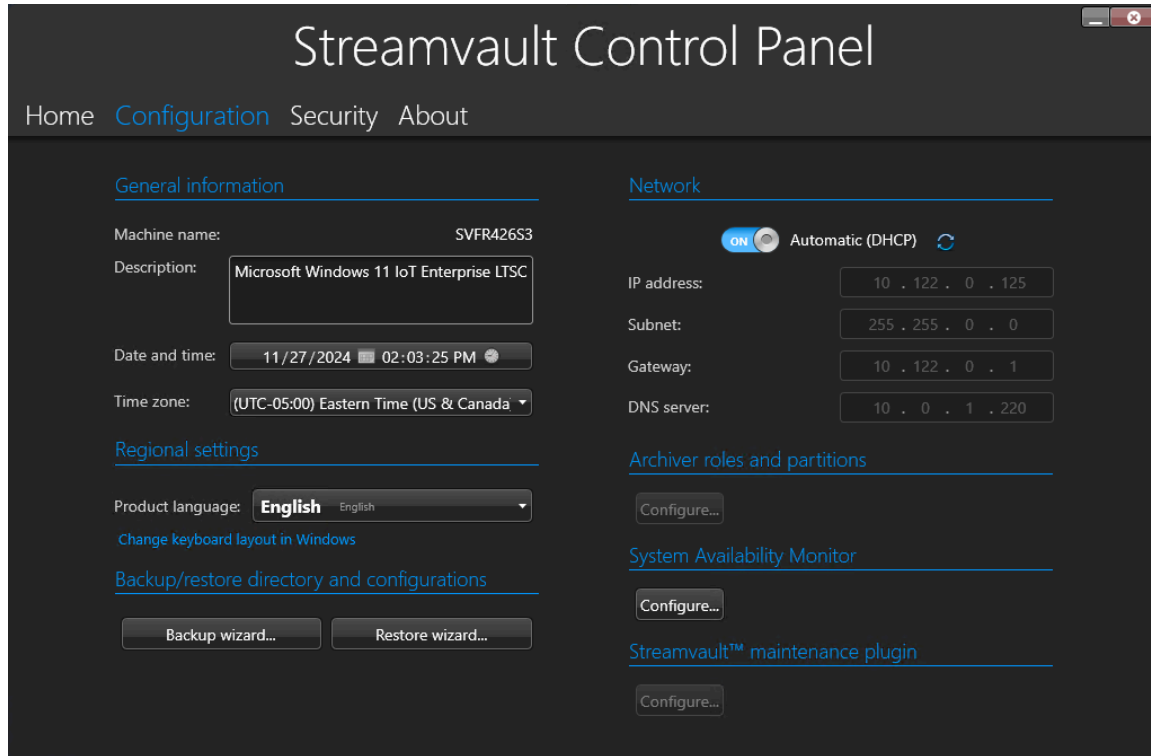
Utilice Genetec Update Service para ayudar a garantizar que los componentes de software de su dispositivo estén actualizados.

Acceso directo al Server Admin

Utilice la aplicación Server Admin para aplicar manualmente una licencia o ver y cambiar la configuración del servidor.

Página de configuración del Panel de Control SV

Utilice la página de *Configuración* del Panel de Control de Streamvault™ para modificar configuraciones generales como las *configuraciones regionales*, *configuraciones de red*, y *configuraciones de System Availability Monitor*.



Para los sistemas que se ejecutan en un servidor de expansión o en modo Cliente, las secciones de *System Availability Monitor* y *Copia de seguridad/restauración de directory y configuraciones* no están disponibles.

Configuración de información general

Use la sección de *Información general* para cambiar configuraciones generales, como el nombre de su dispositivo Streamvault.

- **Nombre de la máquina:** Muestra el nombre de la máquina SV.
- **Descripción:** Introduzca una descripción significativa para ayudar a identificar la máquina.
- **Fecha y hora:** Haga clic en el campo para configurar los valores de fecha y hora que se muestran en la máquina. Alternativamente, puede hacer clic en el ícono del calendario o del reloj que está en el campo para establecer esta configuración.
- **Huso horario:** Seleccione un huso horario de la lista desplegable.

Configuración regional

Use la sección de *Configuraciones regionales* para cambiar la configuración de idioma de la distribución del teclado de su sistema.

- **Idioma del producto:** Seleccione un idioma de la lista para cambiar el idioma de Config Tool y Security Desk.
IMPORTANTE: Para que los cambios surtan efecto, debe reiniciar sus aplicaciones de Security Center.
- **Cambiar la distribución del teclado en Windows:** Haga clic en esta opción para abrir la página de configuración de *Idioma y región* de Windows para cambiar la distribución de su teclado.

IMPORTANTE: Para que los cambios surtan efecto, debe reiniciar su computadora.

NOTA: El SV Control Panel está disponible en inglés, francés y español.

Copia de seguridad y restaurar

Use la sección de *Copia de respaldo/Restauración del Directory y las configuraciones* para tener acceso al asistente de *Copia de respaldo* y al asistente de *Restauración*.

La copia de seguridad y la restauración son características del SV Control Panel. Le permite realizar una copia de seguridad de su base de datos del Directory y de sus archivos de configuración, y luego restaurarlos a la misma ID del sistema. La copia de seguridad y la restauración se pueden usar en caso de una falla del sistema o una actualización de hardware. Esta característica no realiza copias de seguridad de su archivo de licencia, archivos de video u otras bases de datos.

Esta sección no está disponible para sistemas que se ejecutan en un servidor de expansión o en modo Cliente.


- **Asistente de copia de respaldo:** Haga clic en el **Asistente de copia de respaldo** para crear una copia de respaldo de la base de datos de su Directory y de los archivos de configuración.
- **Asistente de Restauración:** Hacer clic **Asistente de restauración** para restaurar una copia de seguridad de su base de datos de Directorio y archivos de configuración en su sistema.

IMPORTANTE: Debe abrir el puerto requerido para asegurarse de que la función de *Copia de Respaldo/Restauración del Directory y las configuraciones* pueda comunicarse con el SV Control Panel. Para obtener más información, consulte [Puertos predeterminados utilizados por Streamvault](#) en la página 4.

Configuración de la red

Use la sección de *Red* para cambiar los ajustes de red, tales como la dirección IP de su dispositivo Streamvault.

- **Automático (DHCP):** De forma predeterminada, el Protocolo de configuración dinámica de host (DHCP) se utiliza para asignar automáticamente la dirección IP, la subred, la puerta de enlace y el servidor DNS. Desactive esta opción si no desea que su servidor DHCP asigne de manera dinámica la dirección IP.

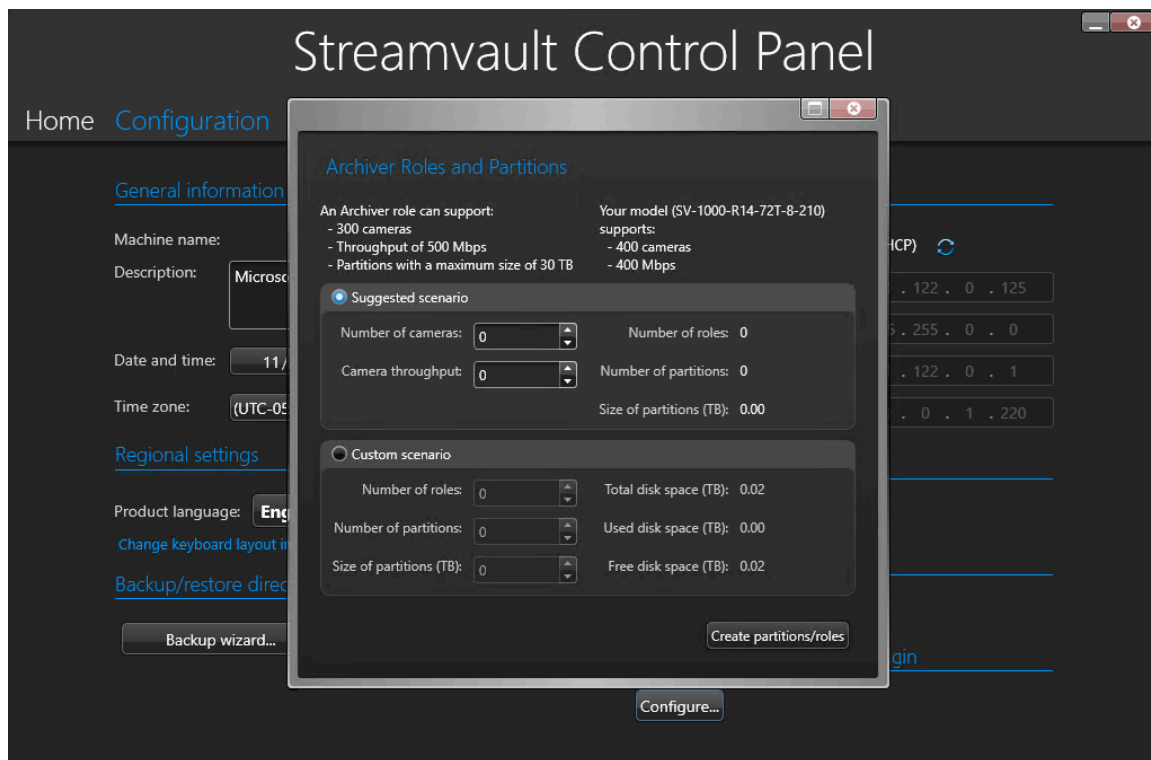
Haga clic en **Actualizar**  para actualizar la configuración de su DHCP y obtener una nueva dirección IP.

- **Dirección IP:** La dirección IP de la máquina.
- **Subred:** La máscara de subred de la máquina.
- **Puerta de enlace:** La dirección IP de la puerta de enlace.
- **Servidor DNS:** La dirección IP del servidor DNS.

Funciones y particiones del Archiver

Utilice la sección de *Funciones y particiones del Archiver* para configurar sistemas que requieren más que el número máximo de cámaras y el rendimiento admitido por un solo Archiver.

Esta sección está disponible para sistemas que ejecutan Security Center 5.9 y versiones posteriores en un servidor de expansión.



- **Una función del Archiver puede admitir:** Muestra la cantidad máxima de cámaras, la cantidad de productividad y el tamaño de partición admitidos por una sola función del Archiver.
- **Su modelo admite lo siguiente:** Muestra la cantidad máxima de cámaras y la cantidad de productividad admitidas por su modelo de dispositivo Streamvault.
- **Escenario sugerido:** Calcula de manera automática la cantidad de funciones, particiones y el tamaño de partición necesarios para el número de cámaras y rendimiento deseados.
- **Escenario personalizado:** Escoja la cantidad de funciones, las particiones y el tamaño de partición deseados para la configuración de sus sistemas.

Para obtener más información sobre el uso de esta función, consulte [Añadir funciones de Archiver en SV Control Panel](#) en la página 39.

Configuración del System Availability Monitor

Use la sección de *System Availability Monitor* para configurar la configuración de System Availability Monitor Agent en su dispositivo Streamvault. Por ejemplo, configurar el método de recopilación de datos y activar el Agente.

También puedes consultar lo siguiente:

- Si el dispositivo se comunica con Security Center
- Cuándo ocurrió el último punto de control
- Qué errores y advertencias recientes se registraron en los registros de Aplicaciones y Servicios

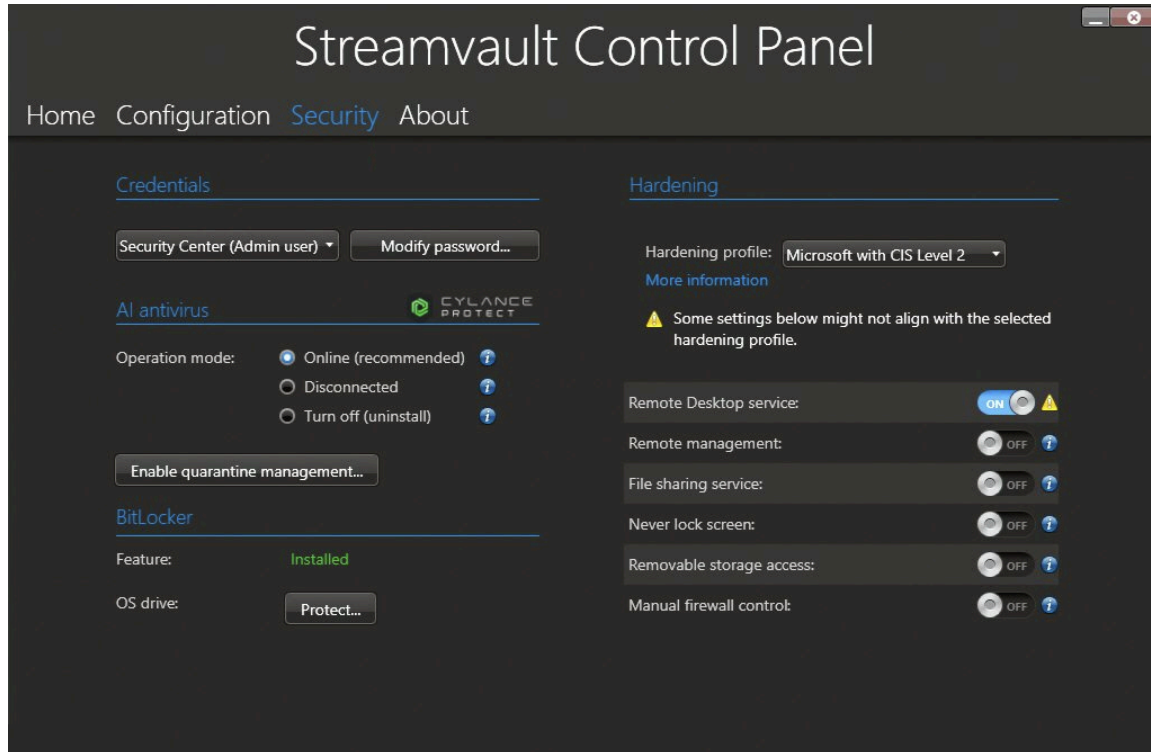
Esta sección no está disponible para sistemas que se ejecutan en un servidor de expansión o en modo Cliente.

Configuración del plugin de Streamvault Maintenance

Utilice la sección de *Plugin de Streamvault Maintenance* para inscribir el plugin en Security Center, si aún no se ha inscrito.

Página de seguridad del SV Control Panel

Utilice la página de *Seguridad* para modificar las contraseñas de los usuarios, elegir el modo de comunicación entre el Agente CylancePROTECT y Genetec™, y aplicar perfiles de endurecimiento y configuraciones de seguridad del sistema a su dispositivo Streamvault™.



Configuraciones de contraseña

Use la sección de *Credenciales* de la página de *Seguridad* para cambiar las contraseñas de las cuentas de usuario para su dispositivo Streamvault.

NOTA: Hay diferentes opciones de contraseña disponibles para el usuario actual en un servidor principal y de expansión. En un servidor de expansión, el administrador solo puede cambiar las contraseñas de Windows, no las contraseñas de las aplicaciones de Security Center.

Defina una contraseña para cada tipo de usuario:

- **Security Center (Usuario administrador):** La contraseña del usuario administrador para Security Desk, Config Tool y Genetec™ Update Service.
- **Administrador del servidor:** La contraseña para la aplicación Genetec™ Server Admin.
- **Operador de Windows:** Haga clic en **Modificar contraseña** para cambiar la contraseña del operador para Windows.

Configuración del antivirus

Use la sección de *Antivirus con IA* para elegir el modo en el que el Agente CylancePROTECT se comunica con Genetec.

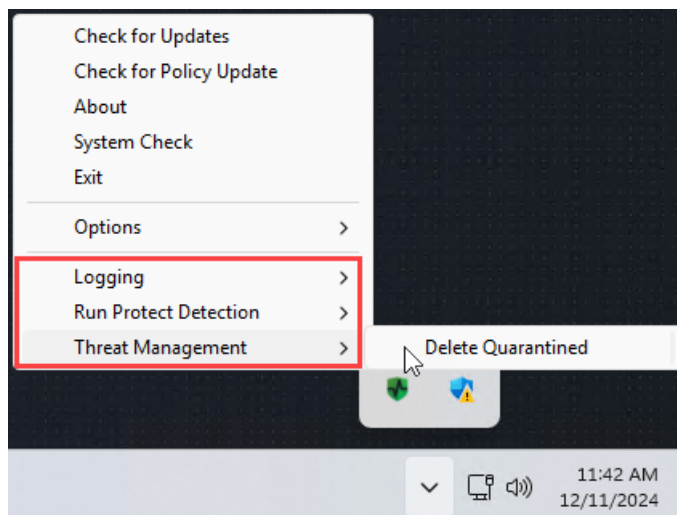
CylancePROTECT es el software antivirus impulsado por IA que se utiliza para la protección y detección de amenazas.

Puede elegir entre los siguientes modos de funcionamiento:

- **En línea (recomendado):** Cuando está en línea, el Agente de CylancePROTECT se comunica con Genetec para informar sobre nuevas amenazas, actualizar su agente y enviar datos para ayudar a mejorar sus modelos matemáticos. Esta opción ofrece el más alto nivel de protección.
- **Desconectado:** El modo de desconexión es para un dispositivo sin conexión a internet. En este modo, CylancePROTECT no puede conectarse ni enviar información a los servicios de gestión de Genetec en la nube. Su dispositivo está protegido contra la mayoría de las amenazas. El mantenimiento y las actualizaciones están disponibles a través de Genetec™ Update Service (GUS).
- **Desactivar:** Seleccione este modo para desinstalar CylancePROTECT de manera permanente de su dispositivo. Su dispositivo utilizará Microsoft Defender para la protección y detección de amenazas de Windows. No recomendamos desactivar CylancePROTECT si el dispositivo no puede recibir actualizaciones de definiciones de virus para Microsoft Defender.

PRECAUCIÓN: Para cambiar de una opción a la otra puede ser necesario reiniciar el equipo, lo que puede ocasionar interrupciones en el sistema.

Haga clic en **Habilitar la administración de cuarentena** para agregar **Administración de amenazas** al menú que se accede haciendo clic derecho del ícono de Cylance en la barra de tareas de Windows. Esta opción le permite eliminar elementos en cuarentena. **Registro y Detección de Protección de Ejecución** también se agregan al menú que se accede haciendo clic derecho. Estas opciones le permiten acceder a registros y activar análisis, de manera respectiva.



Configuraciones de cifrado

Use la sección *BitLocker* para instalar la característica de BitLocker y cifrar la unidad del SO en su dispositivo de Streamvault.

- **Característica:** La característica de BitLocker viene preinstalada en Windows 10 y Windows 11. Si tiene Windows Server, puede hacer clic en **Instalar** para instalar la característica.
- **Disco del sistema operativo:** Haga clic en **Proteger** para cifrar la unidad del SO (C:) con BitLocker. La clave de cifrado se guarda en un chip de Módulo de Plataforma de Confianza (TPM, por sus siglas en inglés) ubicada en la placa del sistema del dispositivo Streamvault. Si se retirara la unidad del SO o se reemplazara el tablero del sistema, se perdería la información de la unidad del SO. La unidad del SO no podría tener acceso a la clave de descifrado del TPM. Puede crear una clave de recuperación que puede usarse para descifrar la unidad en estas situaciones. Sin una clave de descifrado, debe volver a crearse una clave del dispositivo y reinstalarse el software. El cifrado de la unidad del SO también ayuda a proteger la contraseña de administrador de Windows de acceso no autorizado.

Para obtener más información, consulte [Cifrado de la unidad del SO](#).

Configuraciones de endurecimiento

Use la sección de *Endurecimiento* para elegir un perfil de endurecimiento y establecer la configuración de seguridad del sistema para su dispositivo Streamvault.

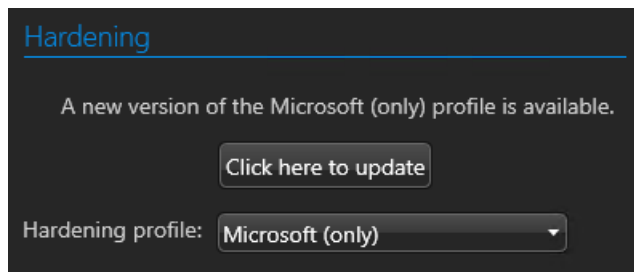
NOTA: Los perfiles de endurecimiento están disponibles solo en aparatos que tengan la [Servicio Streamvault](#). Para obtener más información, consulte [Acerca del servicio Streamvault](#) en la página 15.

Hay cuatro perfiles de endurecimiento predefinidos:

- **Microsoft (solamente):** Este perfil de endurecimiento aplica las líneas base de seguridad de Microsoft a su sistema. Las líneas de base de seguridad de Microsoft son un grupo de configuraciones recomendadas por Microsoft que se basan en los comentarios de los equipos de ingeniería de seguridad, grupos de productos, socios y clientes de Microsoft.
 - **Microsoft con CIS Nivel 1:** Este perfil de endurecimiento aplica las líneas de base de seguridad de Microsoft y el perfil de Nivel 1 (CIS L1) del Centro de seguridad de Internet (CIS) a su sistema. El CIS L1 proporciona requisitos de seguridad esenciales que se pueden implementar en cualquier sistema con poco o ningún impacto en el rendimiento o funcionalidad reducida.
 - **Microsoft con CIS Nivel 2:** Este perfil de endurecimiento aplica las líneas de base de seguridad de Microsoft y los perfiles CIS L1 y Nivel 2 (L2) a su sistema. El perfil CIS L2 ofrece el más alto nivel de seguridad y está destinado a organizaciones donde la seguridad es de suma importancia.
- NOTA:** La estricta seguridad que aporta este perfil de endurecimiento puede reducir la funcionalidad del sistema y dificultar la gestión remota del servidor.
- **Microsoft con STIG:** Este perfil de endurecimiento aplica las líneas de base de seguridad de Microsoft y las Guías de implementación técnica de seguridad (STIG) de la Agencia de Sistemas de Información de Defensa (DISA) a su sistema. Los STIG de DISA se basan en los estándares del Instituto Nacional de Estándares y Tecnología (NIST) y brindan protección de seguridad avanzada para los sistemas Windows del Departamento de Defensa de los EE. UU.

NOTA: De forma predeterminada, todos los dispositivos se envían con el perfil de endurecimiento de Microsoft con CIS Nivel 2 aplicado.

Cuando esté disponible una nueva versión del perfil de endurecimiento seleccionado, aparecerá un botón de **Hacer clic aquí para actualizar**. Haga clic en el botón para instalar la actualización.



Además de los perfiles de endurecimiento, se pueden configurar los siguientes parámetros de seguridad del sistema:

- **Servicio de Escritorio Remoto:** Permita que las personas de su red inicien sesión en el dispositivo mediante una aplicación de *Escritorio remoto*. Para evitar que software malicioso afecte al dispositivo, esta opción está desactivada de forma predeterminada.
- **Administración remota:** Habilite el soporte remoto para las herramientas de administración de Microsoft, como Windows Admin Center, Microsoft Server Manager y PowerShell remoto.
- **Servicio de intercambio de archivos:** Permita que las personas de su red compartan archivos y carpetas que se encuentran en el dispositivo. Para evitar que software malicioso afecte al dispositivo, esta opción está desactivada de forma predeterminada.
- **Nunca bloquee la pantalla:** Si esta opción está activada, Windows mantendrá al usuario conectado, incluso después de 15 minutos de inactividad.
- **Acceso al almacenamiento extraíble:** Habilite el acceso a una llave USB conectada o a un disco duro USB desde Windows.

NOTA: Los usuarios con privilegios administrativos tienen automáticamente acceso al almacenamiento extraíble.

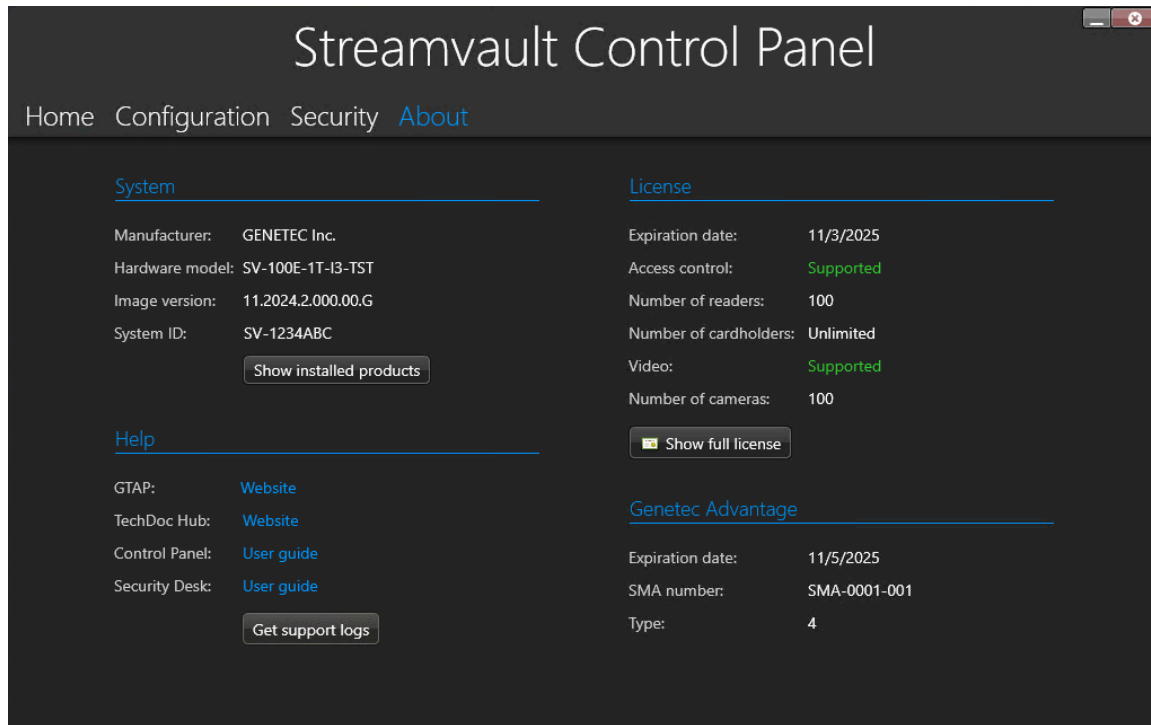
- **Control manual de firewall:** De forma predeterminada, el firewall de Windows Defender usa objetos de política de grupo (GPO) de los perfiles de endurecimiento para proteger el sistema. Active esta opción para controlar las políticas del firewall de forma manual. Todos los GPO se desactivarán.

Para obtener más información, consulte [Cómo desactivar el firewall de Windows](#) en la página 126.

Acerca de la página de SV Control Panel

Use la página de *Acerca de* para ver información útil si necesita asistencia con su dispositivo Streamvault™. La página de *Acerca de* incluye información del sistema, enlaces al Portal de Asistencia Técnica de Genetec™ (GTAP) y documentación del producto, información de la licencia e información del Acuerdo de Mantenimiento de Software (SMA).

Para sistemas que se ejecutan en un servidor de expansión o están en modo Cliente, solo el *Sistema* y *Ayuda* secciones están disponibles.



Información del sistema

Utilice la sección de *Sistema* para ver información sobre el sistema.

- **Fabricante:** Muestra el fabricante del hardware.
- **Modelo de hardware:** Muestra el modelo de hardware.
- **Versión de la imagen:** Muestra la versión de la imagen del software.
- **ID del sistema:** Muestra el número de identificación del sistema.
- **Mostrar productos instalados:** Haga clic para visualizar la versión del software de los componentes de Genetec instalados en el dispositivo.

Información de ayuda

Utilice la sección de *Ayuda* para acceder a los enlaces útiles del GTAP y a la documentación del producto.

- **GTAP:** Haga clic en el enlace para abrir [GTAP](#) y los foros de soporte.
NOTA: Debe tener un nombre de usuario y una contraseña válidos para iniciar sesión en GTAP.
- **Centro de documentos técnicos:** Haga clic en el enlace para abrir el [TechDoc Hub de Genetec](#).
- **Panel de control:** Haga clic en el enlace para abrir la *Guía del usuario del dispositivo Streamvault*, que contiene información del SV Control Panel.
- **Security Desk:** Haga clic en el enlace para abrir la *Guía del usuario de Security Center*.

- **Obtener registros de soporte:** Haga clic para seleccionar los registros de soporte que desea descargar para fines de solución de problemas.

Información de la licencia

Use la sección de *Licencia* para visualizar información acerca de la licencia. La información que se muestra varía en función de las opciones de licencia que tenga.

- **Fecha de caducidad:** Muestra cuándo vence su licencia de Security Center.
- **Control de acceso:** Muestra si las características de control de acceso son compatibles o no.
- **Número de lectores:** Muestra cuántos lectores admite su sistema.
- **Número de tarjetahabientes:** Muestra cuántos tarjetahabientes admite su sistema.
- **Vídeo:** Muestra si las características de vídeo son compatibles o no.
- **Número de cámaras:** Muestra cuántas cámaras admite su sistema.
- **Mostrar licencia completa:** Haga clic para que vea información adicional de la licencia.

Esta sección no está disponible para sistemas que se ejecutan en un servidor de expansión o en modo Cliente.

Información sobre Genetec Advantage

Utilice la sección de *Genetec Advantage* para ver información sobre el SMA.

- **Fecha de caducidad:** Muestra la fecha de vencimiento del Acuerdo de Mantenimiento de Software.
- **Número de SMA:** Muestra el número del SMA.
- **Tipo:** Muestra el tipo de SMA.

Esta sección no está disponible para sistemas que se ejecutan en un servidor de expansión o en modo Cliente.

Recursos adicionales

Esta sección incluye los temas siguientes:

- ["Garantía de producto de su dispositivo Streamvault"](#) en la página 81
- [" Configuración de la contraseña de BIOS "](#) en la página 82
- [" Cambio de la contraseña predeterminada de iDRAC "](#) en la página 85
- ["Cómo agregar un nuevo usuario de iDRAC con privilegios de administrador"](#) en la página 86
- ["Cómo deshabilitar el usuario raíz de iDRAC"](#) en la página 87
- ["Restablecer la imagen de un dispositivo Streamvault"](#) en la página 88
- ["Encontrar la ID del sistema y la versión de la imagen de un dispositivo Streamvault"](#) en la página 89
- ["Permitir compartir archivos en un dispositivo Streamvault"](#) en la página 90
- ["Permitir conexiones a Escritorio Remoto con un dispositivo Streamvault"](#) en la página 91

Garantía de producto de su dispositivo Streamvault

Su dispositivo Streamvault™ está cubierto por una garantía estándar de hardware y software de 3 años, con una extensión opcional de 2 años.

Para obtener una descripción detallada de los términos y condiciones de la garantía del producto Genetec™, consulte la [Descripción general de la garantía del producto Genetec™](#).

Configuración de la contraseña de BIOS

Para proteger los datos de su dispositivo Streamvault™ de acceso no autorizado, debe configurar una contraseña de BIOS.

Lo que debería saber

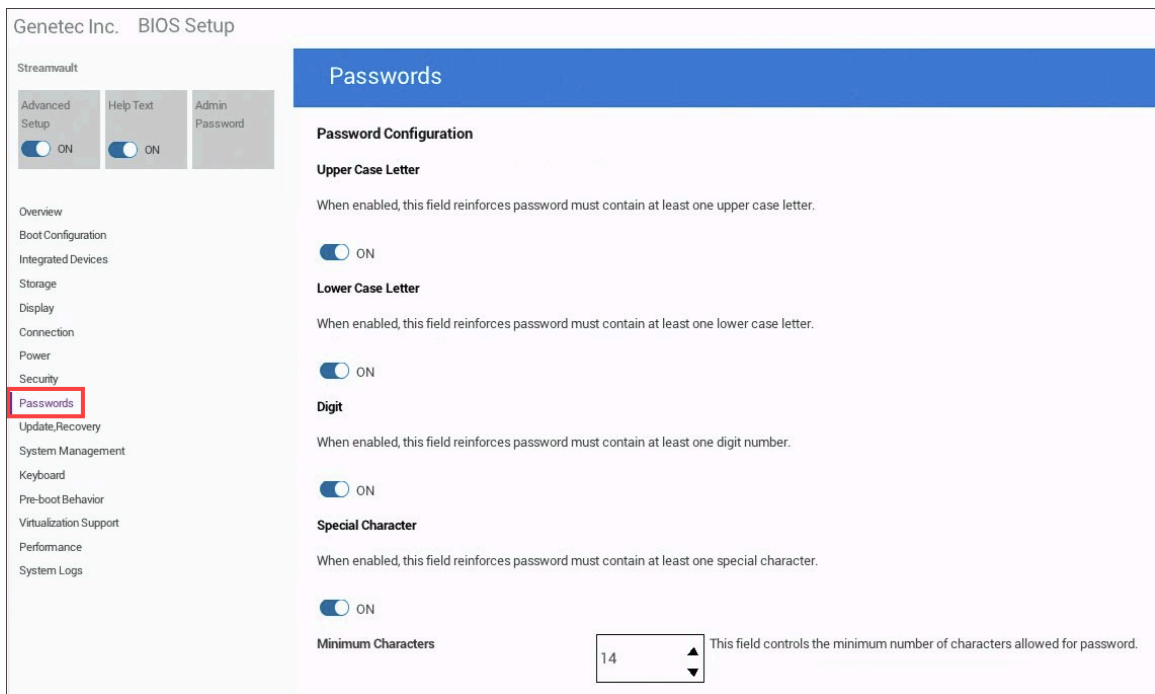
Los pasos para configurar una contraseña de BIOS son diferentes en función del modelo de su dispositivo. Siga el procedimiento aplicable para su dispositivo.

- [Configure la contraseña de BIOS en su dispositivo o estación de trabajo todo en uno Streamvault.](#)
- [Establezca la contraseña de BIOS en su dispositivo SV-1000, SV-2000, SV-4000 o SV-7000 \(PowerEdge\).](#)

Procedimiento

Para configurar la contraseña de BIOS en su dispositivo o estación de trabajo todo en uno Streamvault:

- 1 Encienda o reinicie el dispositivo y presione F2 varias veces hasta que aparezca el menú *Configuración de BIOS*.
- 2 Seleccione **Contraseñas** del menú de la izquierda de la pantalla.
- 3 En la página *Contraseñas*, desplácese hasta la sección *Configuración de contraseñas* y configure los siguientes ajustes:
 - Habilite las opciones **Mayúscula**, **Minúscula**, **Dígitos** y **Caracteres especiales**.
 - Establezca el campo **Caracteres mínimos** en 14.



- Desplácese a la parte superior de la página *Contraseñas* e introduzca una nueva contraseña de BIOS en la sección **Contraseña de administrador**.

Passwords

Admin Password

This field lets you set, change, or delete the administrator (admin) password (sometimes called the "setup" password). The admin password enables several security features. When set, it:

- * Restricts changes to the settings in Setup.
- * Restricts the Legacy boot devices listed in the F12 Boot Menu to those enabled in the "Boot Sequence" field, and restricts the UEFI boot paths listed in the F12 Boot Menu according to the configuration in General/UEFI Boot Path Security.
- * Substitutes for the system password if the system prompts for a password during power on.

Successful changes to this password take effect immediately.

NOTE: If you delete the admin password, the system password, if set, is also deleted. Also, the admin password can be used to delete the HDD password. For this reason, you cannot set an admin password if a system password or HDD password is already set. The admin password must be set first if an admin password is used with the a system password and/or HDD password.

Enter the old password:

Enter the new password and then press <Enter>. Then re-enter the new password and press <Enter> again to confirm.

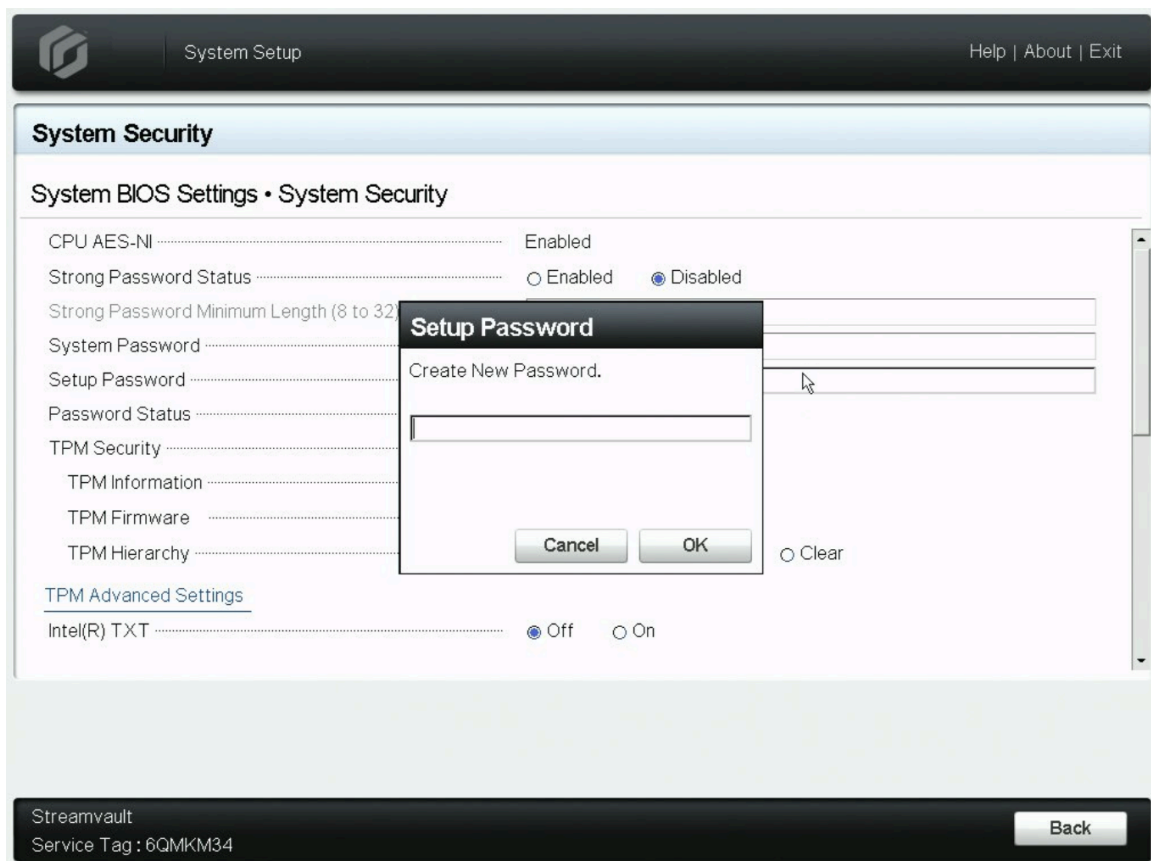
Enter the new password:

- Haga clic en **Salir**.
Se guardan sus cambios y se reinicia el dispositivo.

Para establecer la contraseña de BIOS en su dispositivo SV-1000, SV-2000, SV-4000 o SV-7000, (PowerEdge):

- Encienda o reinicie el dispositivo y presione F2 varias veces hasta que aparezca el menú *Configuración del sistema*.
- En el *Menú principal de configuración del sistema*, haga clic en **BIOS del sistema**.
- En la *Configuración de BIOS del sistema*, haga clic en **Seguridad del sistema**.
- En el campo **Configurar contraseña**, haga clic dentro del cuadro de texto.

- 5 En el cuadro de diálogo *Configurar contraseña* que se abre, introduzca una nueva contraseña y haga clic en **Aceptar**.



- 6 En el campo **Estado de contraseña**, seleccione **Bloqueada** para solicitar que se introduzca la contraseña de configuración antes de cambiar la contraseña del sistema.
- 7 Haga clic en **Atrás > Finalizar > Finalizar**.
Se guardan sus cambios y se reinicia el dispositivo.

Cambio de la contraseña predeterminada de iDRAC

Si su dispositivo Streamvault™ admite iDRAC, se recomienda cambiar de inmediato la contraseña predeterminada de iDRAC para el usuario raíz a fin de prevenir el acceso no autorizado a su dispositivo.

Procedimiento

- 1 Inicie el navegador web Microsoft Edge y visite `https://idrac.local`.
- 2 En la página de inicio de sesión de *Controlador de acceso remoto integrado*, use el nombre de usuario y contraseña predeterminados para iniciar sesión:
 - En **Nombre de usuario**, escriba root.
 - En **Contraseña**, introduzca la contraseña ubicada en la etiqueta de servicio de su dispositivo.
- 3 Después de iniciar sesión, se le pedirá que configure una nueva contraseña para el usuario raíz. Seleccione **Cambiar contraseña predeterminada**, introduzca y confirme la nueva contraseña y haga clic en **Continuar** para guardar sus cambios.

Después de que concluya

Además de cambiar la contraseña predeterminada para el usuario raíz, se recomienda crear un usuario de iDRAC alternativo con privilegios de administrador y deshabilitar el usuario raíz. Para obtener más información, consulte [Cómo agregar un nuevo usuario de iDRAC con privilegios de administrador](#).

Cómo agregar un nuevo usuario de iDRAC con privilegios de administrador

El usuario raíz de iDRAC es conocido y usarlo representa riesgos de seguridad, aunque haya cambiado la contraseña predeterminada. Por lo tanto, es recomendable agregar un nuevo usuario con privilegios de administrador para tener acceso a iDRAC.

Lo que debería saber

Puede agregar un usuario local o usar Microsoft Active Directory para crear una cuenta de usuario.

Procedimiento

- Agregue un usuario nuevo de una de las siguientes formas:
 - Para agregar un usuario local, consulte [Configuración de usuarios locales mediante la interfaz web de iDRAC](#) en la *Guía del usuario de iDRAC* de Dell.
 - Para usar Microsoft Active Directory para crear un nuevo usuario, consulte [Configuración de usuarios de Active Directory](#) en la *Guía del usuario de iDRAC* de Dell.

NOTA: Al configurar los privilegios de usuario, asegúrese de que la **Función de usuario** esté establecida como **Administrador**.

Después de que concluya

Para mayor seguridad, [deshabilite el usuario raíz de iDRAC](#).

Cómo deshabilitar el usuario raíz de iDRAC

Si ha creado un nuevo usuario de iDRAC con privilegios de administrador, deshabilite el usuario raíz para asegurarse de que nadie pueda iniciar sesión con ese nombre de usuario.

Antes de empezar

- [Cambie la contraseña predeterminada de iDRAC en su dispositivo Streamvault.](#)
- [Agregar un nuevo usuario de iDRAC con privilegios de administrador.](#)

Lo que debería saber

Puede deshabilitar el usuario raíz editando los privilegios del usuario.

Procedimiento

- Para obtener detalles sobre cómo editar los privilegios del usuario raíz de iDRAC, consulte [Configuración de usuarios locales mediante la interfaz web de iDRAC](#) en la *Guía del usuario de iDRAC* de Dell.

NOTA: Al editar los privilegios del usuario raíz, asegúrese de configurar lo siguiente:

- Establezca la **Función del usuario** en **Ninguna**.
- Establezca el **Nivel de privilegio de LAN** en **Sin acceso**.
- Establezca el **Nivel de privilegio del puerto serie** en **Sin acceso**.
- Establezca **Serie sobre LAN** en **Deshabilitado**.

Restablecer la imagen de un dispositivo Streamvault

Para volver a restablecer la imagen de un dispositivo Streamvault™, necesita su [Certificado de autenticidad \(COA\)](#) de Microsoft para determinar qué imagen se puede utilizar con el dispositivo. Cada dispositivo Streamvault tiene una etiqueta COA adherida, que indica la edición de Windows que se ejecuta en el dispositivo.

Referirse a [Notas de la versión de Streamvault](#) para obtener una lista de imágenes que son compatibles con su dispositivo, según su edición de Windows. No utilice la imagen de su software si su dispositivo ejecuta una edición de Windows diferente a la indicada en las notas de la versión.

El siguiente es un ejemplo de una etiqueta COA típica con la edición de Windows y la información del certificado estampada. Los productos que contienen versiones embebidas del software de Microsoft tienen una etiqueta COA.



NOTA: Cada imagen de Streamvault está diseñada para funcionar con su respectiva versión de Security Center, como se indica en las [Notas de la Versión de Streamvault](#). Para volver a una versión anterior de Security Center, es posible que sea necesario reducir el nivel de protección del dispositivo.

Para obtener una descripción general de la disponibilidad del producto, el soporte y los servicios disponibles, consulte la [Página del ciclo de vida del producto en GTAP](#).

Encontrar la ID del sistema y la versión de la imagen de un dispositivo Streamvault

Al comunicarse con el Centro de Asistencia Técnica de Genetec™ (GTAC), necesitará la ID del sistema y la versión de la imagen del software de Genetec™ que instaló en el dispositivo.

Antes de empezar

Inicie sesión en Windows como administrador.

Lo que debería saber

Además de la ID del sistema y la versión de la imagen, GTAC podría solicitar el número de certificación y el número de serie. Para encontrar esta información, busque una etiqueta en el dispositivo Streamvault™.

Procedimiento

- 1 Desde el escritorio de Windows, abra **Genetec™ Panel de control SV**.
- 2 Si se le solicita, ingrese la contraseña para el usuario administrador.
- 3 Haga clic en **Acerca de**.
- 4 En la sección de *Sistema*, tome nota de la **ID del sistema** y la **Versión de la imagen**.

Temas relacionados

[Realizar un restablecimiento de fábrica en un dispositivo todo en uno Streamvault](#) en la página 93

[Realizar un restablecimiento de fábrica en un Streamvault estación de trabajo o dispositivo servidor](#) en la página 104

Permitir compartir archivos en un dispositivo Streamvault

Para compartir los archivos y las carpetas de su dispositivo con personas de su red, debe habilitar el uso compartido de archivos en el SV Control Panel.

Antes de empezar

En el dispositivo, inicie sesión en Windows como usuario Administrador.

Lo que debería saber

- Para máxima seguridad, el uso compartido de archivos está deshabilitado de forma predeterminada.
- Las computadoras remotas y su dispositivo deben estar conectados a la misma red IP.

Procedimiento

- 1 En la página de *Seguridad* del SV Control Panel, active la opción de **Servicio de uso compartido de archivos**.
- 2 Hacer clic **Aplicar**.
- 3 Para compartir una carpeta o un archivo con otras personas, haga clic con el botón derecho en una carpeta o un archivo en el Explorador de Archivos de Windows y haga clic en **Compartir**.

Permitir conexiones a Escritorio Remoto con un dispositivo Streamvault

Para controlar un dispositivo desde cualquier computadora o máquina virtual en la red, primero debe habilitar el acceso remoto en el dispositivo.

Antes de empezar

En el dispositivo, inicie sesión en Windows como usuario Administrador.

Lo que debería saber

- Para máxima seguridad, el acceso remoto está deshabilitado de forma predeterminada.
- El dispositivo y la computadora remota deben estar conectados a la misma red.

Procedimiento

- 1 En la página de *Seguridad* del SV Control Panel, encienda la opción de **Servicio de Escritorio Remoto**.
- 2 Hacer clic **Aplicar**.

Temas relacionados

[El Escritorio remoto no se puede conectar a un dispositivo Streamvault](#) en la página 113

Solución de problemas

Esta sección incluye los temas siguientes:

- [" Realizar un restablecimiento de fábrica en un dispositivo todo en uno Streamvault "](#) en la página 93
- ["Realizar un restablecimiento de fábrica en un Streamvault estación de trabajo o dispositivo servidor"](#) en la página 104
- ["Los controladores Mercury EP permanecen fuera de línea cuando TLS 1.1 está desactivado"](#) en la página 109
- ["Habilitación de la seguridad de la capa de transporte \(TLS\)"](#) en la página 110
- ["El Escritorio remoto no se puede conectar a un dispositivo Streamvault"](#) en la página 113
- ["Cómo eliminar restricciones de cuentas de usuarios que no son administradores"](#) en la página 117
- ["Las cuentas locales no pueden acceder al Escritorio remoto, al servicio de uso compartido de archivos y a la administración remota "](#) en la página 118
- ["Habilitación de servicios relacionados con Tarjetas Inteligentes"](#) en la página 119
- ["Habilitación de la compatibilidad con controladores Mercury EP y LP firmware 1.x.x"](#) en la página 120
- ["Habilitación del soporte para la integración de Synergis IX"](#) en la página 122
- ["Modificación de GPO locales para cuentas de usuarios no administradores"](#) en la página 123
- ["Cómo desactivar el firewall de Windows"](#) en la página 126

Realizar un restablecimiento de fábrica en un dispositivo todo en uno Streamvault

Si el software de un dispositivo Streamvault™ Todo en Uno no se inicia o deja de funcionar como se esperaba, puede realizar un restablecimiento de fábrica utilizando una memoria USB.

Antes de empezar

- [Haga una copia de seguridad de su base de datos de Directly en SV Control Panel](#)
- Tenga la licencia correcta para la versión de Security Center que desea restaurar o instalar.
- Tener el ID del sistema y la contraseña que le enviaron por correo electrónico cuando compró el electrodoméstico. Ver [Encontrar la ID del sistema y la versión de la imagen de un dispositivo Streamvault](#) en la página 89.
- (Recomendado) Conecte su dispositivo a Internet mediante una conexión Ethernet por cable para que el sistema pueda validar la conectividad.
NOTA: Si no hay una conexión a internet disponible, fallará la validación, pero podrá continuar utilizando su dispositivo.

Lo que debería saber

Un restablecimiento de fábrica elimina y sobrescribe todos los datos que se encuentran actualmente en la unidad de Windows (C:), incluidas las bases de datos y los registros. Los archivos de video en otras unidades no se ven afectados.

Procedimiento

- 1 [Cree una memoria USB de restablecimiento de fábrica que contenga la imagen del software.](#)
- 2 [Usando la llave USB, restablezca la imagen en su dispositivo.](#)

Después de que concluya

[Reconfigure su dispositivo.](#)

Temas relacionados

[Encontrar la ID del sistema y la versión de la imagen de un dispositivo Streamvault](#) en la página 89

Crear una memoria USB con restablecimiento de fábrica para un dispositivo Streamvault Todo en Uno

Antes de poder restablecer la imagen de un dispositivo Streamvault™ Todo en Uno, debe preparar una memoria USB de arranque que contenga la imagen del software Streamvault requerida.

Antes de empezar

- Consigue una llave USB con al menos 32 GB de almacenamiento. Algunas memorias USB no pueden iniciar la imagen; Si esto ocurre, intente utilizar una marca o modelo de llave diferente.
PRECAUCIÓN: Todos los datos de la llave USB se eliminan cuando crea una unidad de arranque.





Procedimiento

- 1 Comuníquese con el [Centro de Asistencia Técnica de Genetec™](#) (GTAC, por sus siglas en inglés) para obtener la imagen de recuperación.

La imagen de recuperación viene en uno de los siguientes tres formatos:

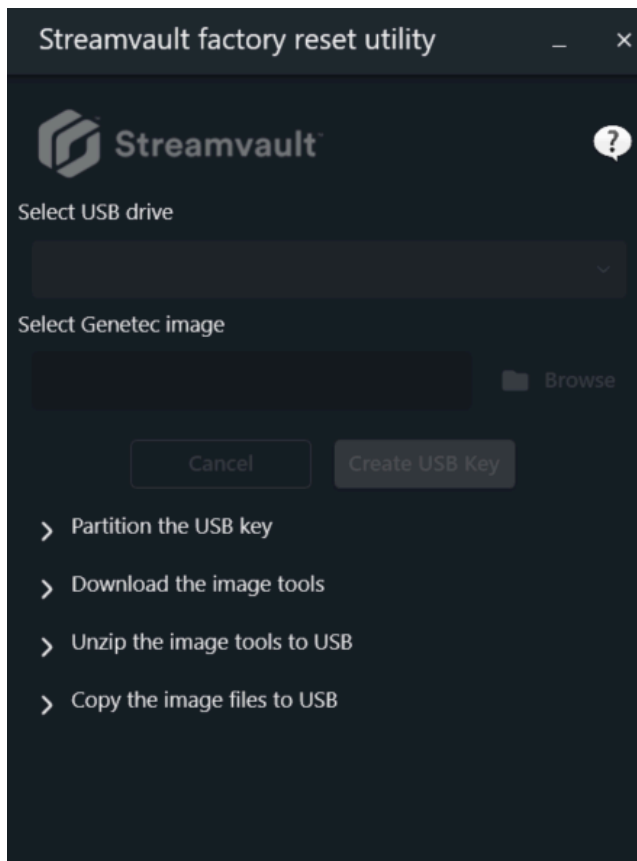
- Un archivo *.zip* que contiene archivos *.swm*.
- Un archivo *.iso* que contiene los archivos *.swm* y la interfaz de usuario de la *Utilidad de restablecimiento de fábrica de Streamvault*, que utilizará para restablecer la imagen del software.
- Un archivo de *.iso* que contiene el asistente de *configuración de Windows*, que usará para restablecer la imagen del software.

- 2 Si su imagen de recuperación es un archivo *.zip*, descomprima el contenido en cualquier carpeta de Windows.
- 3 Desde la página de [Descarga de Productos](#) del GTAP, descargue el creador de USB de la *Utilidad de restablecimiento de fábrica de Streamvault*.
 - a) Desde el *Buscador de descargas* lista, seleccione su versión de Security Center.
 - b) Desde la lista de *Otros*, descargue el paquete de *Utilidad de Restablecimiento de Fábrica de Streamvault*.

Other	
Genetec Video Player	
Streamvault All-in-One image for Windows 11 LTSC (SHA1: D399117267BDC481D70E5A713711C1F4DB6C7A7D)	
Streamvault Control Panel 3.1.0	
Streamvault Factory Reset Utility	

- 4 Inserte la memoria USB en un puerto USB.
- 5 Abra el creador de USB de la *Utilidad de restablecimiento de fábrica de Streamvault* que descargó de TechDoc Hub.

- 6 Desde el **Seleccionar unidad USB** lista, seleccione una llave USB que tenga al menos 32 GB de almacenamiento.



- 7 En la sección de *Seleccionar la imagen de Genetec*, haga clic en **Examinar** y seleccione el archivo `.swm` o `.iso` que descargó.

NOTA: Si necesita un archivo `.swm`, seleccione cualquiera de los archivos descomprimidos de la carpeta `wim`. Todos los archivos `.swm` de esa carpeta se copiarán a la memoria USB.

- 8 Haga clic en **Crear memoria USB**.

El *Utilidad de restablecimiento de fábrica de Streamvault* comienza a particionar la llave USB, descargar las herramientas de imagen y copiar los archivos de imagen.

Cuando se completa la descarga, se muestra el siguiente mensaje: La memoria USB se creó con éxito.

El siguiente video muestra cómo crear una memoria USB con restablecimiento de fábrica con un archivo `.iso`.



Después de que concluya

Restablezca la imagen de software de su Dispositivo todo en uno Streamvault .

Restablecer la imagen del software en un dispositivo todo en uno

Una vez que haya preparado una memoria USB de arranque que tenga la imagen del software Streamvault™ necesaria, puede usarla para restablecer la imagen del software en un dispositivo Streamvault todo en uno.

Antes de empezar

- [Asegúrese de tener la llave USB que contiene el software de recuperación para su dispositivo.](#)

Lo que debería saber

- El restablecimiento demora entre 20 y 30 minutos; durante este período se ejecutan varios scripts y el dispositivo se reinicia varias veces.
- No interrumpa el proceso de reinicio. Cerrar o apagar el dispositivo de forma manual puede dañar la recuperación.

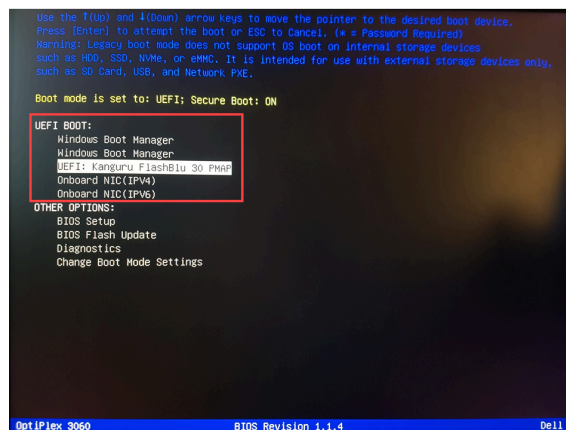
Procedimiento

Para restablecer la imagen del software:

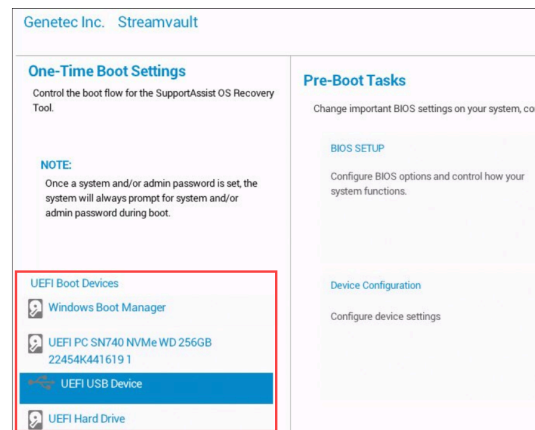
- 1 Apague el aparato.
- 2 Introduzca la memoria USB que creó en un puerto USB.
- 3 Encienda el dispositivo y presione F12 varias veces hasta que aparezca el menú de arranque. En función de su dispositivo, se abre el menú de arranque UEFI o el menú de arranque único de Streamvault.

- 4 Seleccione la memoria USB y presione Entrar.

NOTA: La apariencia de su menú de arranque puede verse diferente.



UEFI Boot menu



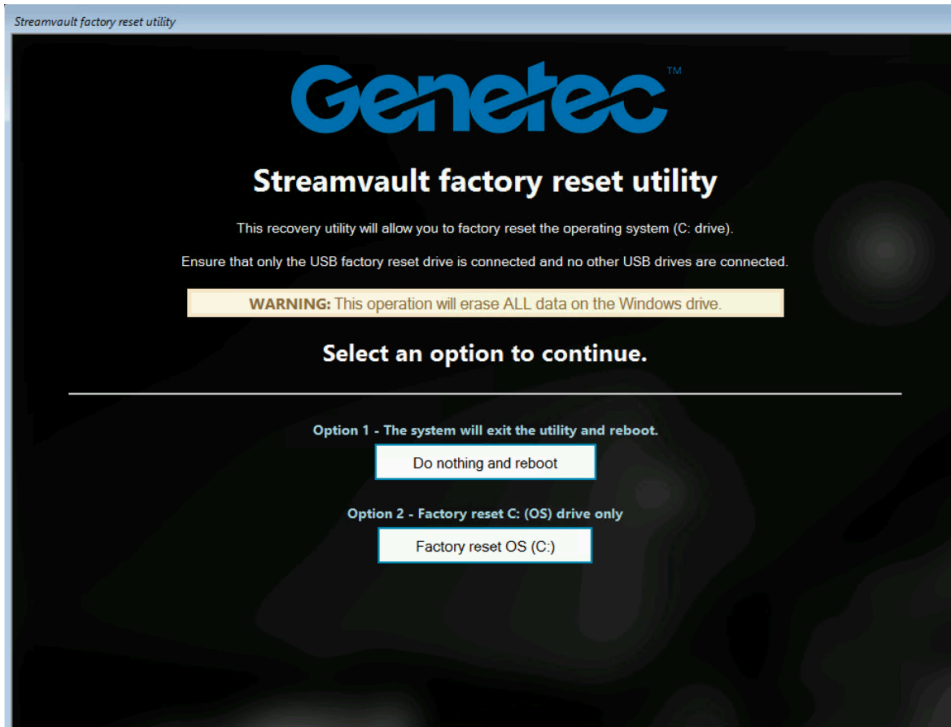
Streamvault One-time Boot menu

En función de la imagen del software, se abre la *Utilidad de restablecimiento de fábrica de Streamvault* o el asistente de *Configuración de Windows*.

- 5 Restablezca la imagen del software con la herramienta que corresponda a su dispositivo:
 - [Utilidad de restablecimiento de fábrica de Streamvault](#)
 - [Asistente de Configuración de Windows](#)

Para restablecer la imagen del software utilizando la Utilidad de restablecimiento de fábrica de Streamvault:

- 1 Cuando la memoria USB arranque en modo de recuperación, seleccione **Restablecer sistema operativo de fábrica (C:)** para formatear y reinstalar la unidad del sistema del dispositivo.



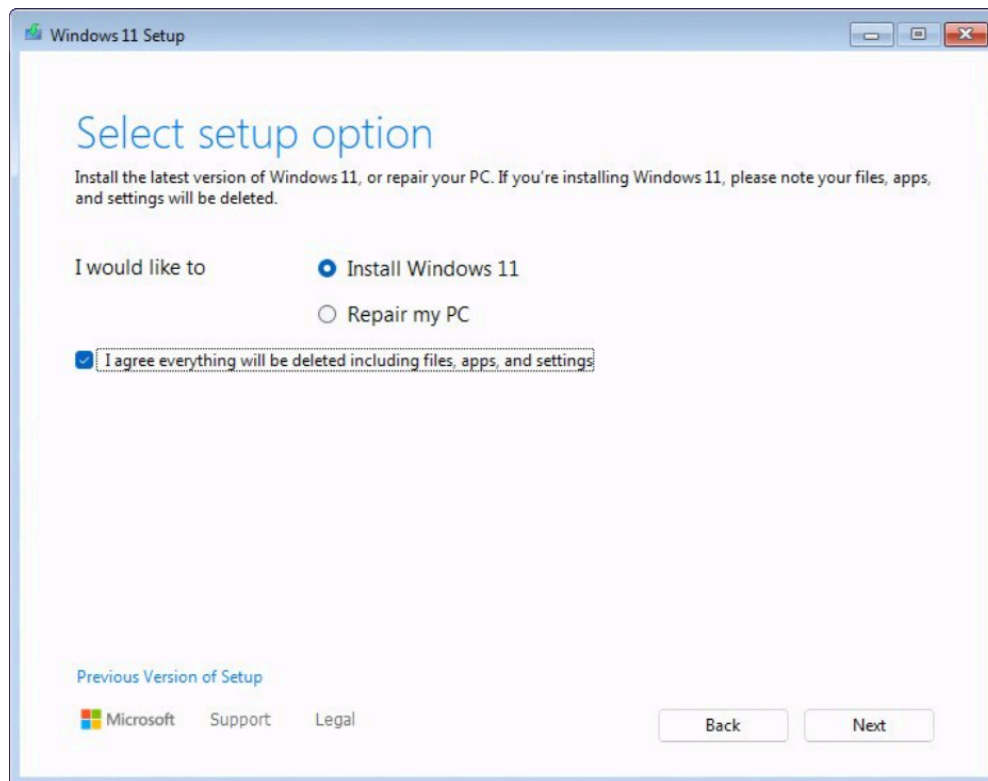
- 2 Cuando se le solicite, escriba Yes (Sí) y pulse Enter. Espere a que se complete el restablecimiento de fábrica.
- 3 Cuando se complete el restablecimiento de fábrica, retire la memoria USB del dispositivo y pulse Entrar para reiniciar.
- 4 En el cuadro de diálogo del *Validador de Producto de Genetec™*, introduzca el número de pieza (N.º de Producto) del dispositivo y el número de serie de Genetec™. Estos números se pueden encontrar en la etiqueta de Genetec ubicada en la parte superior del electrodoméstico. Si no hay ninguna etiqueta, puede ingresar cualquier texto para continuar. Aparece el botón **Iniciar**.
- 5 Haga clic en **Iniciar**. Se muestra uno de los siguientes mensajes de estado:
 - **APROBADO:** El proceso fue exitoso. Continúe con el siguiente paso.
 - **APROBADO: sin transmisión:** El proceso fue exitoso; sin embargo, la conexión a Internet no estaba disponible en ese momento. Continúe con el siguiente paso.
 - **DESAPROBADO:** El proceso no fue exitoso. Comuníquese con el [Centro de Asistencia Técnica de Genetec™](#)
- 6 Si recibes un PASA o PASA - Sin transmisión mensaje, cierre el *Validador de productos Genetec™* ventana.
- 7 Espere a que se cierre la secuencia de comandos en segundo plano y luego reinicie el dispositivo.

Para restablecer la imagen del software mediante el asistente de Configuración de Windows:

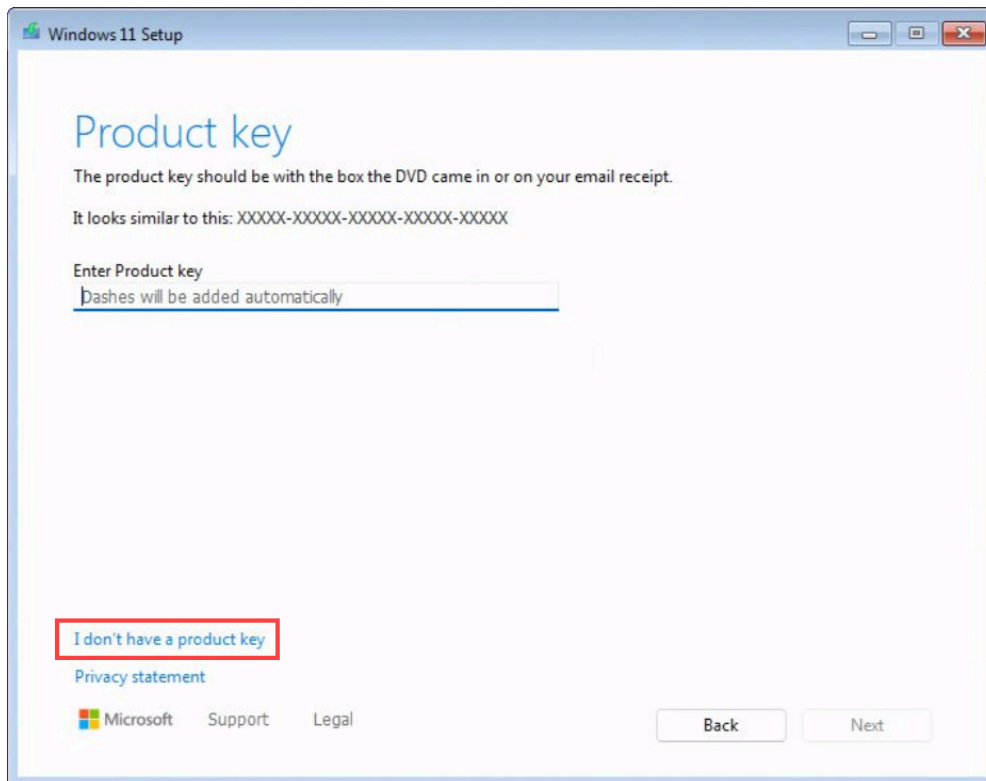
- 1 En la pantalla de *Seleccionar configuración de idioma*, seleccione su configuración de idioma y hora preferidos y haga clic en **Siguiente**.
- 2 En la pantalla de *Seleccionar configuración del teclado*, seleccione su teclado preferido y haga clic en **Siguiente**.

- 3 En la pantalla de *Seleccionar opción de configuración*, seleccione **Instalar Windows X**, donde X representa la versión de Windows que está instalando. Acepte que sus archivos, aplicaciones y configuraciones se eliminarán y haga clic en **Siguiente**.

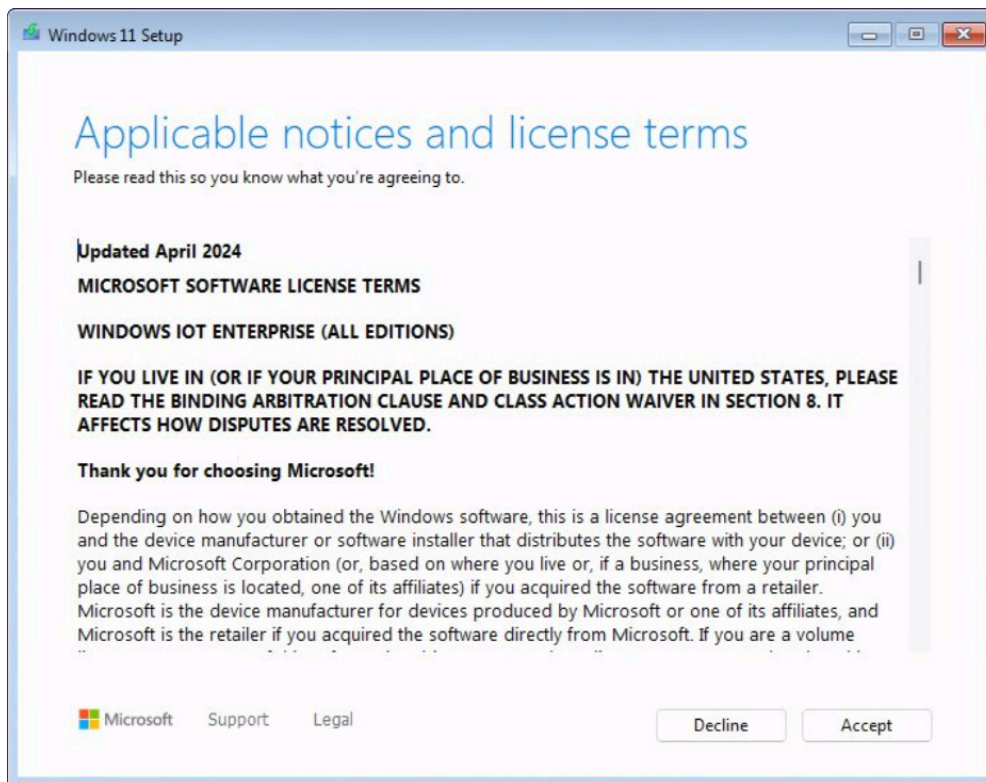
NOTA: Los archivos de video almacenados en el disco de video secundario no se ven afectados. Solo se eliminan los archivos en el disco del sistema operativo.



- 4 En la pantalla de *Clave de producto*, realice una de las siguientes acciones:
- Si el dispositivo está conectado a Internet, haga clic en **No tengo una clave de producto** para continuar. El dispositivo recupera de manera automática sus datos de activación de Microsoft.
 - Si el dispositivo no está conectado a Internet, introduzca la clave de licencia que se encuentra en la etiqueta del [Certificado de Autenticidad \(COA\)](#) colocada en el dispositivo y haga clic en **Siguiente**.



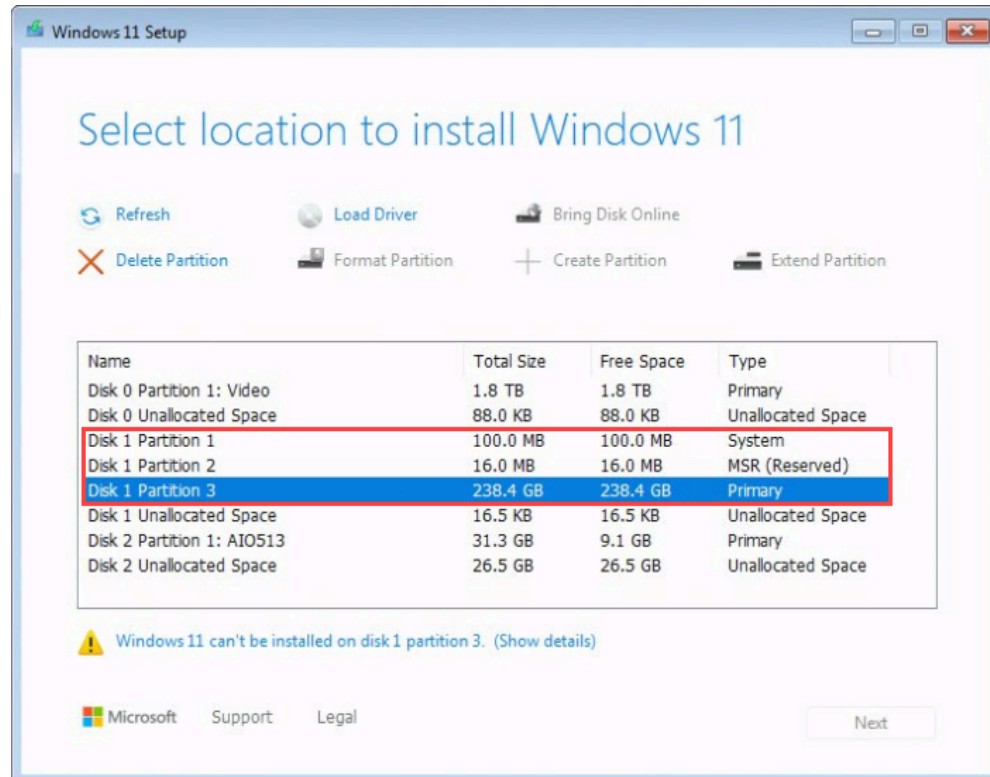
- 5 En la pantalla de *Avisos aplicables y términos de la licencia*, lea los términos de la licencia y haga clic en **Aceptar**.



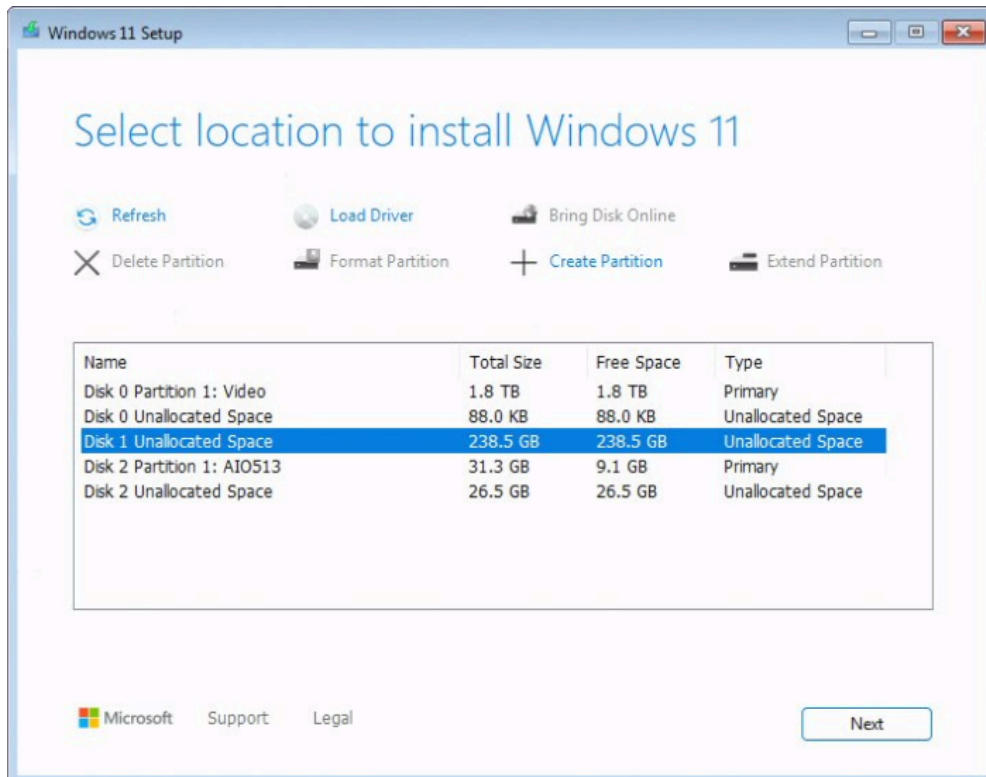
- 6 En la pantalla de *Seleccionar ubicación para instalar Windows X*, elimine las particiones principal, del sistema y MSR (si corresponde) del SO.

Solo quedará espacio sin asignar en el disco del SO, y el asistente de configuración de Windows recreará de forma automática las particiones eliminadas durante el proceso de instalación.

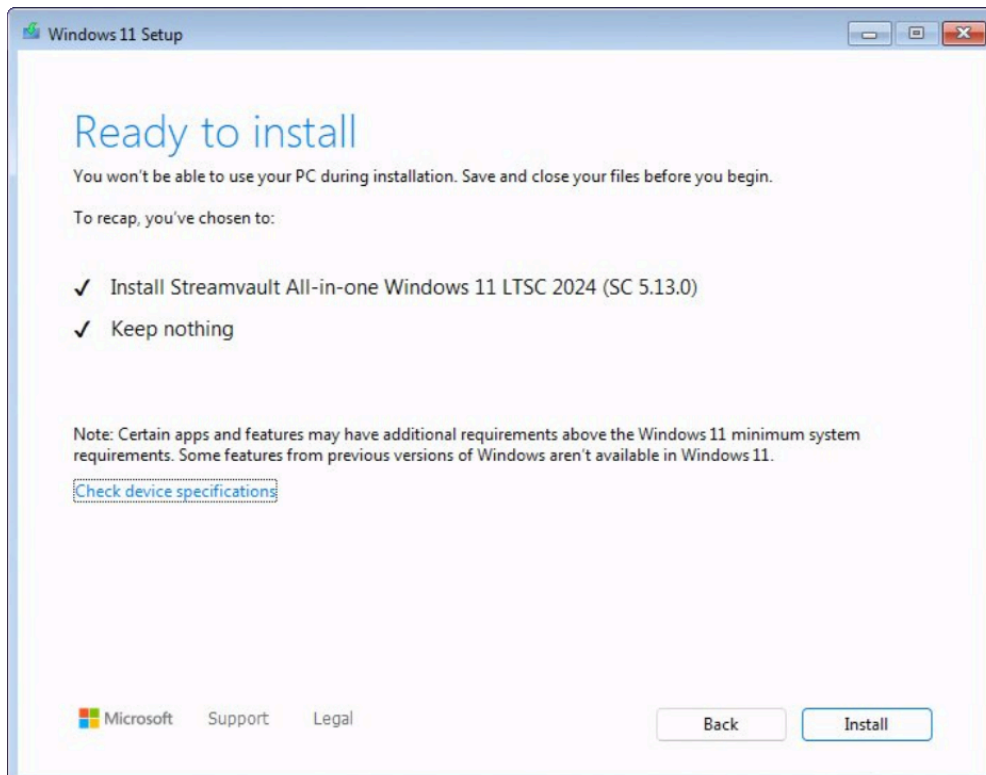
PRECAUCIÓN: Por lo general, la partición principal del disco del SO tiene un tamaño inferior a 1 TB. No elimine la partición principal del disco de almacenamiento de video, donde se almacenan sus archivos de video.



- 7 Seleccione el espacio no asignado en el disco del SO y haga clic en **Siguiente**.



- 8 En la pantalla de *Listo para instalar*, haga clic en **Instalar**.



- 9 Cuando se completa la instalación, el sistema se reinicia en Windows y se ejecuta de manera automática un script para finalizar la instalación. Cuando el script haya terminado de ejecutarse, reinicie el dispositivo.

Mire este video para aprender cómo restablecer la imagen del software en un dispositivo Todo en Uno usando un USB de arranque que contiene archivos *.swm*.



Después de que concluya

- Inicie sesión en Windows utilizando el nombre de usuario y la contraseña predeterminados que se encuentran en la etiqueta adherida al dispositivo.
- [Active su licencia de Security Center](#).
- Si realizó una copia de respaldo de las configuraciones de Security Center antes de llevar a cabo el restablecimiento a valores de fábrica, [restaure las configuraciones a través de SV Control Panel](#).
- [Reconfigure su dispositivo](#).

Realizar un restablecimiento de fábrica en un Streamvault estación de trabajo o dispositivo servidor

Si el software de su servidor o estación de trabajo Streamvault™ no se enciende o deja de funcionar según lo previsto, puede realizar un restablecimiento de fábrica con una memoria USB.

Antes de empezar

- Haga una copia de seguridad de toda la configuración de Security Center utilizando el Panel de control de SV. Para más información, ver [Crear una copia de respaldo de la base de datos de su Directory](#) en la página 37.
- Consigue una llave USB con al menos 32 GB de almacenamiento. Algunas memorias USB no pueden iniciar la imagen; Si esto ocurre, intente utilizar una marca o modelo de llave diferente.
PRECAUCIÓN: Todos los datos de la llave USB se eliminan cuando crea una unidad de arranque.
- Tenga la licencia correcta para la versión de Security Center que desea restaurar o instalar.
- Tener el ID del sistema y la contraseña que le enviaron por correo electrónico cuando compró el electrodoméstico.

Lo que debería saber

- **Se aplica a:** Todos los modelos que comienzan con SVW, SVR y SVA, y todos los servidores con números de modelo SV-1000E y superiores.
- Para electrodomésticos todo en uno, consulte [Realizar un restablecimiento de fábrica en un dispositivo todo en uno Streamvault](#) en la página 93.
- Un restablecimiento de fábrica elimina todos los datos que se encuentran en la actualidad en la unidad del Sistema (SO), pero no afecta la configuración predeterminada de fábrica de la unidad RAID.
- El restablecimiento puede fallar si las unidades de disco duro, las unidades RAID o las particiones del dispositivo se cambiaron de la configuración predeterminada de fábrica. En tal caso, comuníquese con el [Centro de asistencia técnica Genetec™ \(GTAC\)](#).

Procedimiento

- 1 [Crear una llave USB de restablecimiento de fábrica.](#)
- 2 [Usando la llave USB, restablezca la imagen en su dispositivo.](#)

Después de que concluya

[Configura tu electrodoméstico.](#)

Temas relacionados

[Encontrar la ID del sistema y la versión de la imagen de un dispositivo Streamvault](#) en la página 89

Crear una memoria USB de restablecimiento de fábrica para una estación de trabajo o dispositivo de servidor Streamvault

Antes de poder restablecer la imagen de una estación de trabajo o dispositivo de servidor Streamvault™, debe preparar una memoria USB de arranque que contenga la imagen de software de Streamvault requerida.

Antes de empezar

Consigue una llave USB con al menos 32 GB de almacenamiento. Algunas memorias USB no pueden iniciar la imagen; Si esto ocurre, intente utilizar una marca o modelo de llave diferente.

PRECAUCIÓN: Todos los datos de la llave USB se eliminan cuando crea una unidad de arranque.





Procedimiento

- 1 Comuníquese con el [Centro de Asistencia Técnica de Genetec™ \(GTAC, por sus siglas en inglés\)](#) para obtener la imagen de recuperación.

La imagen de recuperación viene en uno de los siguientes tres formatos:

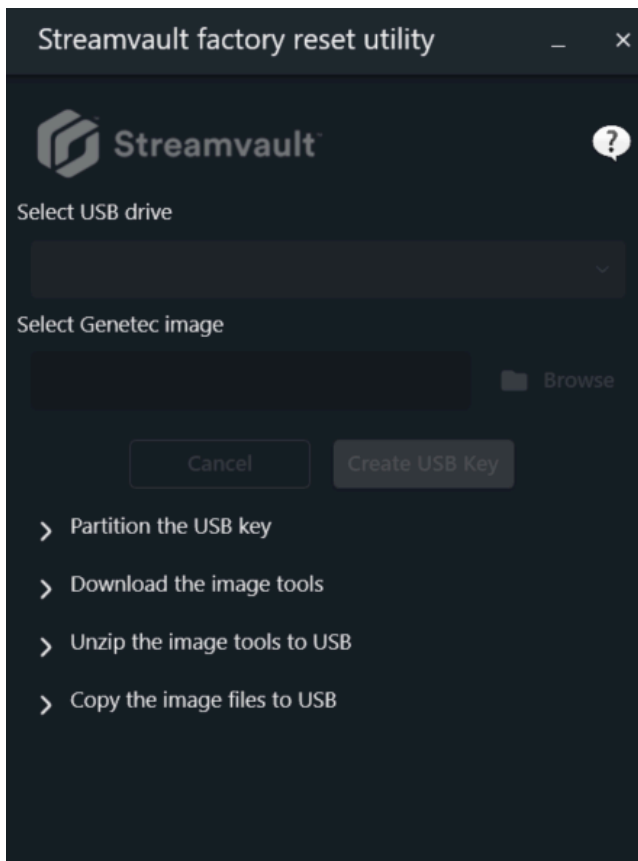
- Un archivo *.zip* que contiene archivos *.swm*.
- Un archivo *.iso* que contiene los archivos *.swm* y la interfaz de usuario de la *Utilidad de restablecimiento de fábrica de Streamvault*, que utilizará para restablecer la imagen del software.
- Un archivo de *.iso* que contiene el asistente de *configuración de Windows*, que usará para restablecer la imagen del software.

- 2 Si su imagen de recuperación es un archivo *.zip*, descomprima el contenido en cualquier carpeta de Windows.
- 3 Desde la página de [Descarga de Productos](#) del GTAP, descargue el creador de USB de la *Utilidad de restablecimiento de fábrica de Streamvault*.
 - a) Desde el *Buscador de descargas* lista, seleccione su versión de Security Center.
 - b) Desde la lista de *Otros*, descargue el paquete de *Utilidad de Restablecimiento de Fábrica de Streamvault*.

Other	
Genetec Video Player	
Streamvault All-in-One image for Windows 11 LTSC (SHA1: D399117267BDC481D70E5A713711C1F4DB6C7A7D)	
Streamvault Control Panel 3.1.0	
Streamvault Factory Reset Utility	

- 4 Inserte la memoria USB en un puerto USB.
- 5 Abra el creador de USB de la *Utilidad de restablecimiento de fábrica de Streamvault*.

- 6 Desde el **Seleccionar unidad USB** lista, seleccione una llave USB que tenga al menos 32 GB de almacenamiento.



- 7 En la sección de *Seleccionar la imagen de Genetec*, haga clic en **Examinar** y seleccione el archivo `.swm` o `.iso` que descargó.

Si necesita un archivo `.swm`, seleccione la imagen requerida de la carpeta *<número de etiqueta de servicio>*.

- 8 Haga clic en **Crear memoria USB**.

El *Utilidad de restablecimiento de fábrica de Streamvault* comienza a particionar la llave USB, descargar las herramientas de imagen y copiar los archivos de imagen.

Cuando se completa la descarga, se muestra el siguiente mensaje: La memoria USB se creó con éxito.

El siguiente video muestra cómo crear una memoria USB con restablecimiento de fábrica con un archivo `.iso`.



Después de que concluya

[Restablezca la imagen del software de su estación de trabajo o dispositivo servidor Streamvault](#) .

Restablecer la imagen del software en una Streamvault estación de trabajo o un dispositivo servidor

Una vez que haya preparado una memoria USB de arranque que tenga la imagen de software requerida Streamvault™, puede usarla para restablecer la imagen de software en una estación de trabajo o dispositivo servidor.

Antes de empezar

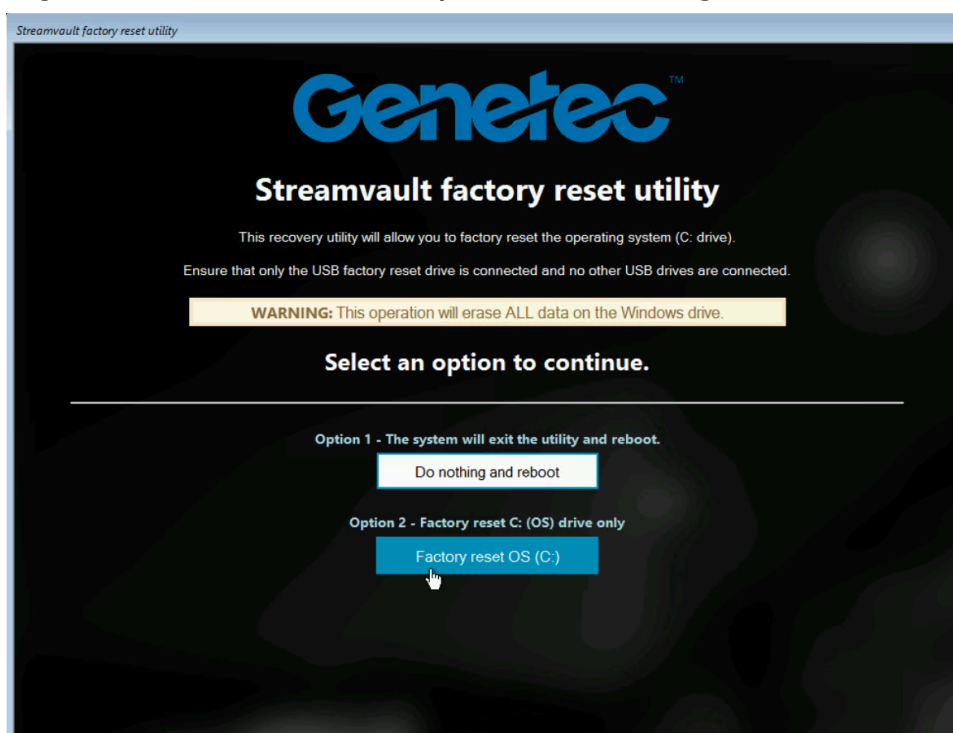
- [Asegúrese de tener la llave USB que contiene el software de recuperación para su dispositivo.](#)

Lo que debería saber

- El restablecimiento no afecta los ajustes predeterminados de fábrica de la unidad RAID.
- El restablecimiento puede fallar si los discos duros, las unidades RAID o las particiones del dispositivo han cambiado desde la configuración predeterminada de fábrica. En tal caso, comuníquese con el [Centro de asistencia técnica Genetec™ \(GTAC\)](#).

Procedimiento

- 1 Apague el aparato.
- 2 Introduzca la memoria USB de arranque que creó en un puerto USB.
- 3 Encienda el dispositivo Streamvault.
- 4 Cuando se le solicite, pulse F12.
Se abre el *Administrador de Arranque*. Haga clic en **One-shot UEFI Boot Menu**.
- 5 Seleccione su memoria USB y presione Entrar.
Se abre *la utilidad de restablecimiento de fábrica de Streamvault*.
- 6 Haga clic en **Restablecer el sistema operativo (C:) a la configuración de fábrica**.



Se abre un símbolo del sistema y la *Utilidad de restablecimiento de fábrica de Streamvault* analiza el sistema para detectar la unidad del sistema (OS).

- 7 En el Símbolo del Sistema, escriba Yes para confirmar que se detectó el disco duro correcto y pulse Entrar para iniciar el restablecimiento a valores de fábrica.

IMPORTANTE: No interrumpa, apague ni reinicie la estación de trabajo durante el proceso de redigitalización. Puede tardar hasta 20 minutos, dependiendo de la velocidad de su memoria USB.

- 8 Cuando se haya completado el restablecimiento de fábrica, pulse la tecla Enter cuando se le solicite para reiniciar la estación de trabajo.
- 9 Retire la memoria USB del puerto USB.

La estación de trabajo ya se ha restablecido a su estado predeterminado.

Mire este video para aprender cómo restablecer la imagen del software en una estación de trabajo o dispositivo de servidor Streamvault.



Después de que concluya

- Inicie sesión en Windows utilizando el nombre de usuario y la contraseña predeterminados que se encuentran en la etiqueta adherida al dispositivo.
- [Active su licencia de Security Center.](#)
- Si realizó una copia de respaldo de las configuraciones de Security Center antes de llevar a cabo el restablecimiento a valores de fábrica, [restaure las configuraciones a través de SV Control Panel.](#)
- [Reconfigure su dispositivo.](#)

Los controladores Mercury EP permanecen fuera de línea cuando TLS 1.1 está desactivado

Después de registrar un controlador Mercury EP en Security Center, la unidad no se conecta.

No recibe ningún error ni advertencia sobre este problema.

Se aplica a:

- Streamvault™ SV-100E 16.3 y versiones posteriores
- Streamvault™ SV-300E 16.3 y versiones posteriores
- Streamvault™ SV-350E 16.3 y versiones posteriores

Causa

Todos los controladores Mercury EP requieren el protocolo Transport Layer Security (TLS) 1.1 para comunicarse con Security Center. Sin embargo, el protocolo está deshabilitado en todos los dispositivos Streamvault™ Todo en Uno de la versión 16.3 y posteriores.

Solución

[Habilitar Transport Layer Security 1.1.](#)

Habilitación de la seguridad de la capa de transporte (TLS)

Los protocolos Transport Layer Security (TLS) 1.0 y 1.1 tienen varias vulnerabilidades importantes, por lo que están deshabilitados en dispositivos Streamvault™. Cuando un dispositivo inscrito en Security Center requiere uno de estos protocolos para la comunicación, debe habilitar el protocolo en su dispositivo.

Lo que debería saber

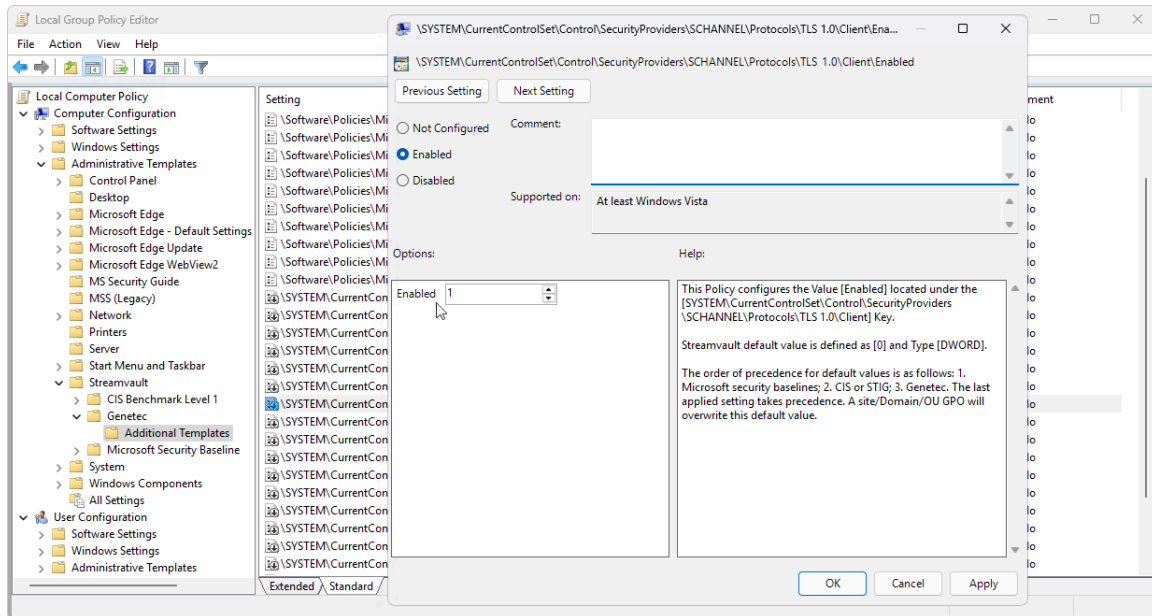
- TLS 1.1 está deshabilitado en la imagen 16.3 y posteriores del software Streamvault.
- TLS 1.0 está deshabilitado en la imagen del software Streamvault 16.0 y posteriores.
- Solo habilite la versión de TLS que requiere su dispositivo.
- Habilite TLS en los nodos del servidor (entrante) y del cliente (saliente).
- Por razones de seguridad, las opciones de Propiedades de Internet están deshabilitadas en los dispositivos. Si su dispositivo tiene el servicio Streamvault, puede habilitar Transport Layer Security desde el Editor de Políticas de Grupo Local. Si su dispositivo no tiene el servicio Streamvault, solo puede habilitar Transport Layer Security desde el Editor del Registro de Windows.

Procedimiento

Para habilitar Transport Layer Security en un dispositivo con el servicio Streamvault:

- 1 Abra el símbolo del sistema como administrador y ejecute `gpedit.msc`.
Se abre el Editor de Políticas de Grupo Local.
- 2 Ir a **Configuración de la Computadora > Plantillas Administrativas > Streamvault > Genetec > Plantillas Adicionales**.
- 3 Habilitar Transport Layer Security 1.*n* en el cliente, donde *n* representa el número de versión menor:
 - a) Haga clic derecho en `\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.n\Client\Enabled` y haga clic en **Editar**.
 - b) Coloque **Activado** en 1 y haga clic en **Aplicar > ACEPTAR**.
 - c) Haga clic derecho en `\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.n\Client\DisabledByDefault` y haga clic en **Editar**.
 - d) Coloque **DisabledByDefault** en 0 y haga clic en **Aplicar > ACEPTAR**.

- 4 Habilitar Transport Layer Security 1.n en el servidor:
 - a) Haga clic derecho en `\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.0\Server\Enabled` y haga clic en **Editar**.
 - b) Coloque **Activado** en 1 y haga clic en **Aplicar** > **ACEPTAR**.
 - c) Haga clic derecho en `\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.0\Server\DisabledByDefault` y haga clic en **Editar**.
 - d) Coloque **DisabledByDefault** en 0 y haga clic en **Aplicar** > **ACEPTAR**.

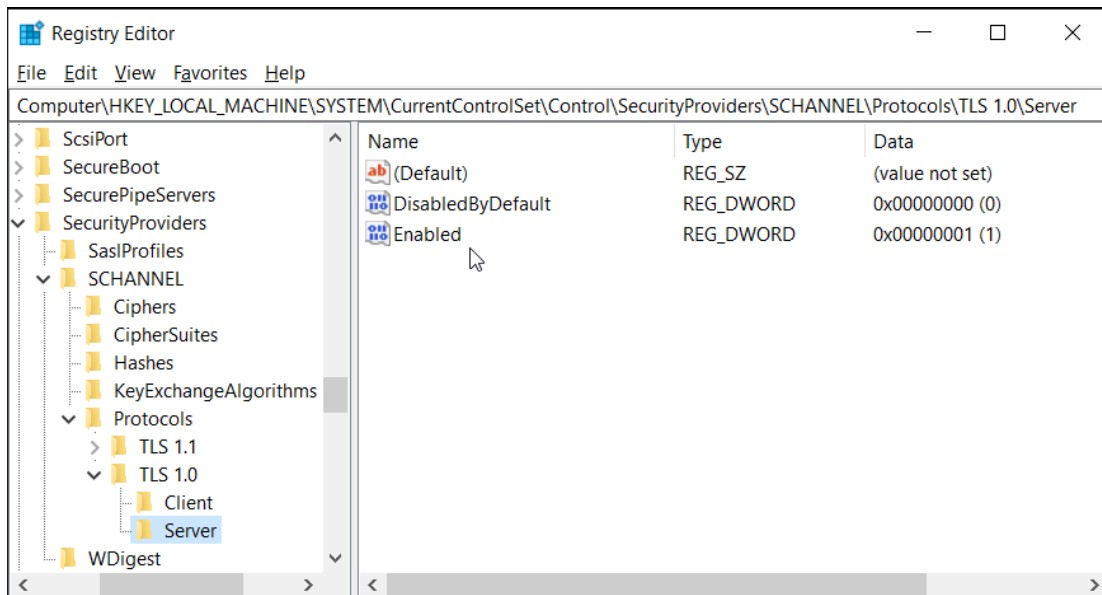


- 5 Reinicie Windows.

Para habilitar Transport Layer Security en un dispositivo sin el servicio Streamvault:

- 1 Abra el Editor del Registro de Windows.

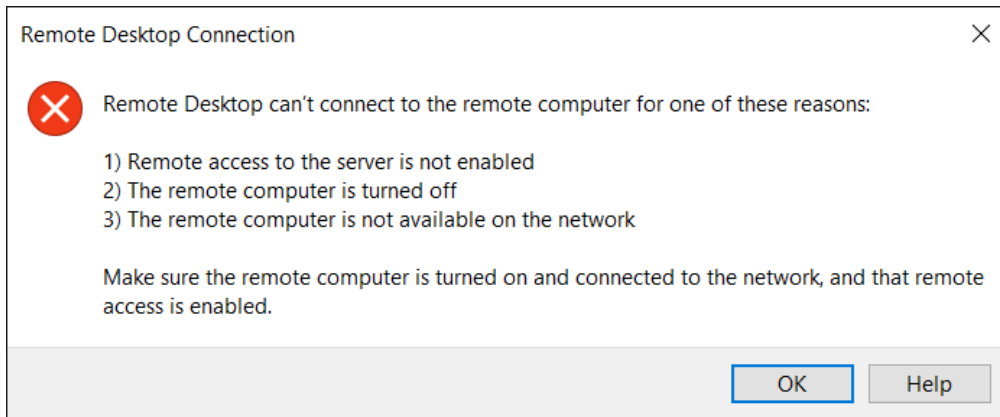
- 2 Habilite TLS 1.*n*, donde *n* representa el número de versión menor:
 - a) Vaya a `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.n`.
 - b) Seleccione el nodo de **Servidor**, establezca **DisabledByDefault** en 0 y establezca **Activado** en 1.
 - c) Seleccione el nodo de **Cliente**, establezca **DisabledByDefault** en 0 y establezca **Activado** en 1.



- 3 Reinicie Windows.

El Escritorio remoto no se puede conectar a un dispositivo Streamvault

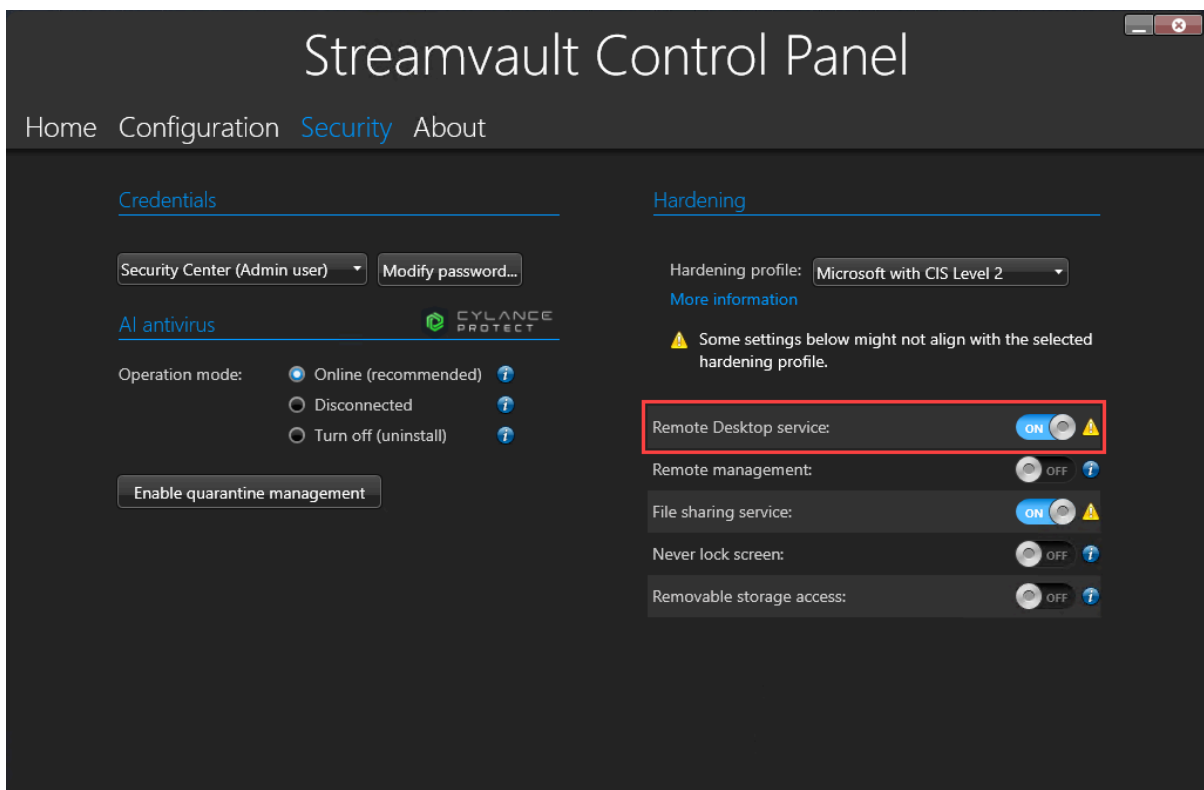
Cuando intenta acceder a un dispositivo Streamvault™ mediante el Escritorio remoto, recibe un mensaje que indica que el Escritorio remoto no puede conectarse a la computadora remota.



El servicio de Escritorio remoto está deshabilitado en SV Control Panel

Descripción: Para garantizar la máxima seguridad, el acceso remoto está deshabilitado de forma predeterminada en un dispositivo.

Solución: [Habilitar el acceso remoto en el dispositivo](#). En la página de *Seguridad* del SV Control Panel, active el **Servicio de Escritorio remoto**.



El escritorio remoto no está permitido en Windows

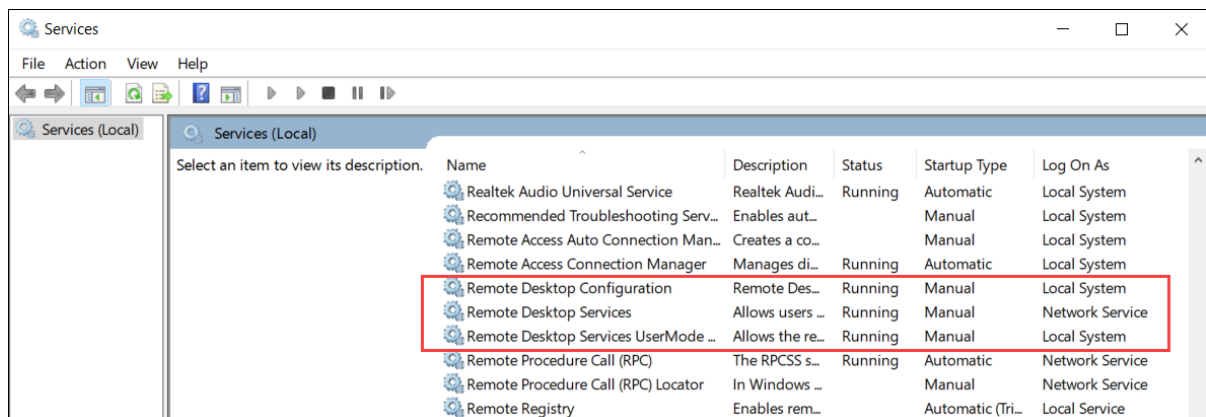
Descripción: Aunque el **Servicio de Escritorio remoto** está activado en SV Control Panel, esta configuración no está permitida en Windows.

Solución: Sobrescriba la configuración de Windows apagando y volviendo a encender la opción de **Servicio de Escritorio remoto**.

Los servicios de Escritorio Remoto no se están ejecutando

Descripción: Los Servicios de Escritorio remoto se detuvieron en Windows.

Solución: Abra la consola de Servicios de Windows, asegúrese de que **Servicios de Escritorio Remoto** haya iniciado sesión como un usuario de **Servicio de Red**, y asegúrese de que los otros servicios de Escritorio Remoto se estén ejecutando.

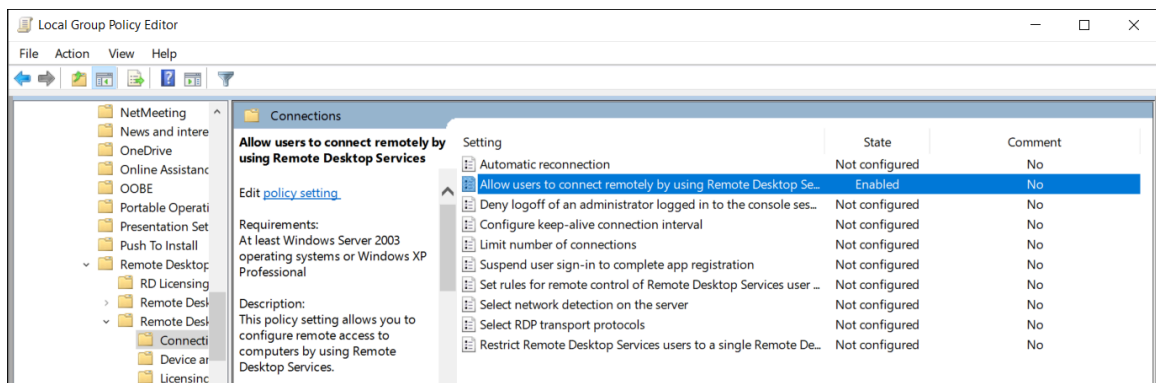


Se deniegan los servicios de escritorio remoto

Descripción: Windows está configurado para denegar el acceso de los usuarios remotos a los Servicios de Escritorio Remoto.

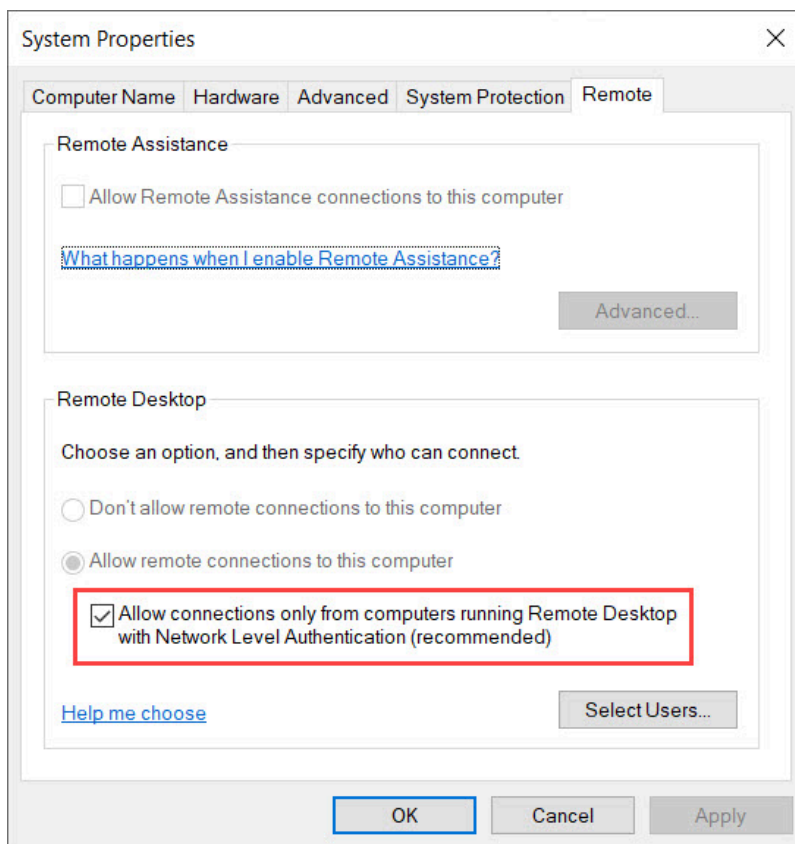
Solución: Permita el acceso de usuarios remotos al dispositivo mediante los Servicios de Escritorio Remoto:

1. Abra el símbolo del sistema como administrador y ejecute `gpedit.msc`.
2. Vaya a **Configuración de la Computadora > Plantillas Administrativas > Componentes de Windows > Servicios de Escritorio Remoto > Host de Sesión de Escritorio Remoto > Conexiones**.
3. Habilite la opción de **Permitir que los usuarios se conecten de forma remota mediante los Servicios de Escritorio Remoto**.



4. En el símbolo del sistema, ejecute `gpupdate / fuerza`.

- Desde el Panel de control de Windows, vaya a **Sistema y Seguridad > Permitir acceso remoto**.
Se abre la ventana de *Propiedades del Sistema* en la pestaña de **Remoto**.
- En la sección de *Escritorio Remoto*, asegúrese de que **Permitir conexiones solo desde computadoras que ejecutan Escritorio Remoto con Autenticación de Nivel de Red (recomendado)** está seleccionado.



Las políticas de grupo local niegan el acceso remoto

Descripción: Las directivas de grupo locales de Windows están configuradas para denegar el acceso remoto a su dispositivo.

Solución: Configure las directivas de grupo en su dispositivo para permitir el acceso remoto:

- Abra el símbolo del sistema como administrador y ejecute `gpedit.msc`.
- Vaya a **Configuración de la Computadora > Configuración de Windows > Configuración de Seguridad > Políticas Locales > Asignaciones de Derechos de Usuario**.
- Verifique la siguiente configuración de la política de grupo:
 - Permitir el inicio de sesión a través de Servicios de Escritorio Remoto** se debe establecer en **Administradores**.
 - Denegar el acceso a esta computadora desde la red** se debe establecer en **Invitados**.
 - Denegar el inicio de sesión a través de Servicios de Escritorio Remoto** se debe establecer en **Invitados**.

La autenticación NTLMv2 no es compatible

Descripción: El dispositivo o la computadora remota no admite la autenticación NTLMv2.

NOTA: Si todas las computadoras cliente admiten NTLMv2, Microsoft y varias organizaciones independientes recomiendan la política de *Enviar solo respuestas NTLMv2*. Consulta con Microsoft [Seguridad de la red: nivel de autenticación de LAN Manager](#) mejores prácticas y consideraciones de seguridad antes de cambiar la configuración.

Solución: Para asegurarse de que su entorno permite la autenticación NTLMv2:

1. Abra el símbolo del sistema como administrador y ejecute `gpedit.msc`.
2. Vaya a **Configuración de la Computadora > Configuración de Windows > Configuración de Seguridad > Políticas locales > Opciones de Seguridad > Seguridad de red: nivel de autenticación del Administrador de LAN**.
3. Configure la política para **Enviar LM y NTLM - usar la seguridad de sesión NTLMv2 si se negocia**.

Contáctenos

Solución: Si la Conexión a Escritorio Remoto aún no puede conectarse, [comuníquese con el Centro de Asistencia Técnica de Genetec \(GTAC\)](#).

Temas relacionados

[Permitir conexiones a Escritorio Remoto con un dispositivo Streamvault](#) en la página 91

Cómo eliminar restricciones de cuentas de usuarios que no son administradores

De forma predeterminada, las cuentas de usuarios que no son administradores, incluido el Operador, tienen acceso limitado a las funciones del Panel de Control de Streamvault™. Puede eliminar las restricciones de esas cuentas para que tengan más acceso a las funciones.

Antes de empezar

- Si una persona inicia sesión como Administrador, puede eliminar las restricciones de las cuentas que no sean de administrador.
- Las restricciones solo se pueden eliminar en sistemas con el servicio Streamvault.

Procedimiento

- 1 Abra el Explorador de archivos y navegue hasta *C:\Windows\System32\GroupPolicyUsers*.
- 2 Elimine la carpeta *S-1-5-32-545* y todo su contenido. Esta carpeta contiene las restricciones para los no administradores.
- 3 Reinicie Windows.

Las cuentas locales no pueden acceder al Escritorio remoto, al servicio de uso compartido de archivos y a la administración remota

Cuando las opciones de **Servicio de Escritorio Remoto**, **Administración Remota**, o **Servicio de uso compartido de archivos** están activadas en SV Control Panel, pero las cuentas locales aún no pueden acceder a las funciones.

Este comportamiento se aplica a los productos de Windows Server que tienen SV Control Panel 3.0 y versiones posteriores:

- Serie Streamvault™ SV-1000E
- Serie Streamvault™ SV-2000E
- Serie Streamvault™ SV-4000EX
- Serie Streamvault™ SV-7000EX

De forma predeterminada, el servicio de Escritorio remoto, la Administración remota y el Servicio de uso compartido de archivos están deshabilitados para el administrador local y las cuentas locales, como el Operador. Con las versiones anteriores del SV Control Panel, el administrador local y las cuentas locales tenían acceso a estas funciones cuando estaban activadas. A partir de SV Control Panel 3.0, solo el administrador local tiene acceso cuando las funciones están activadas.

Este nuevo comportamiento se controla a través de la política de seguridad de **Denegar el acceso a esta computadora desde la red** y cumple con la línea de base de seguridad de Microsoft para Windows Server.

Habilitación de servicios relacionados con Tarjetas Inteligentes

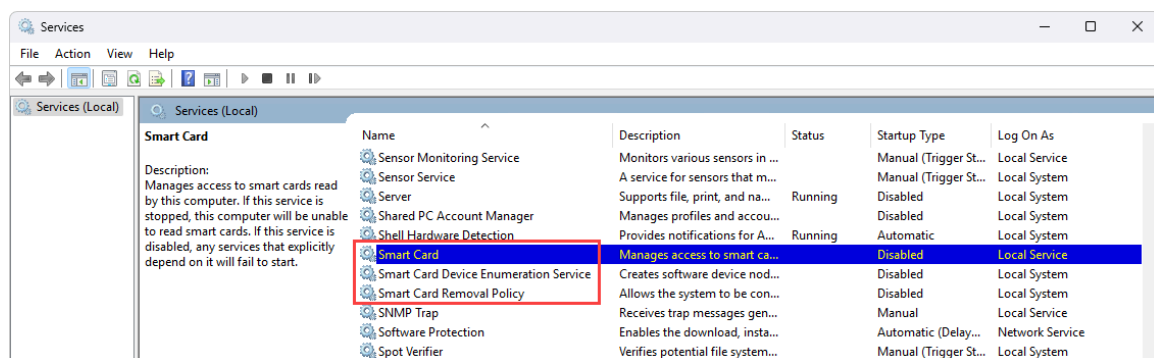
Si ha actualizado a SV Control Panel 3.0 desde una versión anterior y desea habilitar los servicios relacionados con la Tarjeta Inteligente, puede hacerlo a través de la aplicación Servicios de Windows.

Lo que debería saber

La opción de **Habilitar la compatibilidad con Tarjetas Inteligentes** no está disponible en SV Control Panel 3.0, ya que los servicios de Tarjeta Inteligente están habilitados de forma predeterminada.

Procedimiento

- 1 En Windows, ejecute *servicios.msc* para abrir la aplicación de *Servicios*.
- 2 Habilitar el servicio de **Tarjeta Inteligente**.
 - a) Haga clic derecho en el servicio de **Tarjeta Inteligente** y seleccione **Propiedades**.
Se abre el cuadro de diálogo de *Propiedades*.
 - b) En la pestaña de **General**, localice el campo de **Tipo de inicio** y seleccione **Automático**.
 - c) Haga clic en **Aplicar** > **Aceptar**.
- 3 Habilitar el **Servicio de Enumeración de Dispositivos de Tarjetas Inteligentes**.
 - a) Haga clic derecho en **Servicio de Enumeración de Dispositivos de Tarjetas Inteligentes** y seleccione **Propiedades**.
Se abre el cuadro de diálogo de *Propiedades*.
 - b) En la pestaña de **General**, localice el campo de **Tipo de inicio** y seleccione **Manual**.
 - c) Haga clic en **Aplicar** > **Aceptar**.
- 4 Habilitar el **Servicio de Enumeración de Dispositivos de Tarjetas Inteligentes**.
 - a) Haga clic derecho en el servicio de **Política de Eliminación de Tarjetas Inteligentes** y seleccione **Propiedades**.
Se abre el cuadro de diálogo de *Propiedades*.
 - b) En la pestaña de **General**, localice el campo de **Tipo de inicio** y seleccione **Manual**.
 - c) Haga clic en **Aplicar** > **Aceptar**.



Habilitación de la compatibilidad con controladores Mercury EP y LP firmware 1.x.x

Antes de poder integrar controladores Mercury EP o LP firmware 1.x.x en su dispositivo Streamvault™, debe habilitar un conjunto de cifrado de Capa de Puertos Seguros (SSL, por sus siglas en inglés) más antiguo.

Lo que debería saber

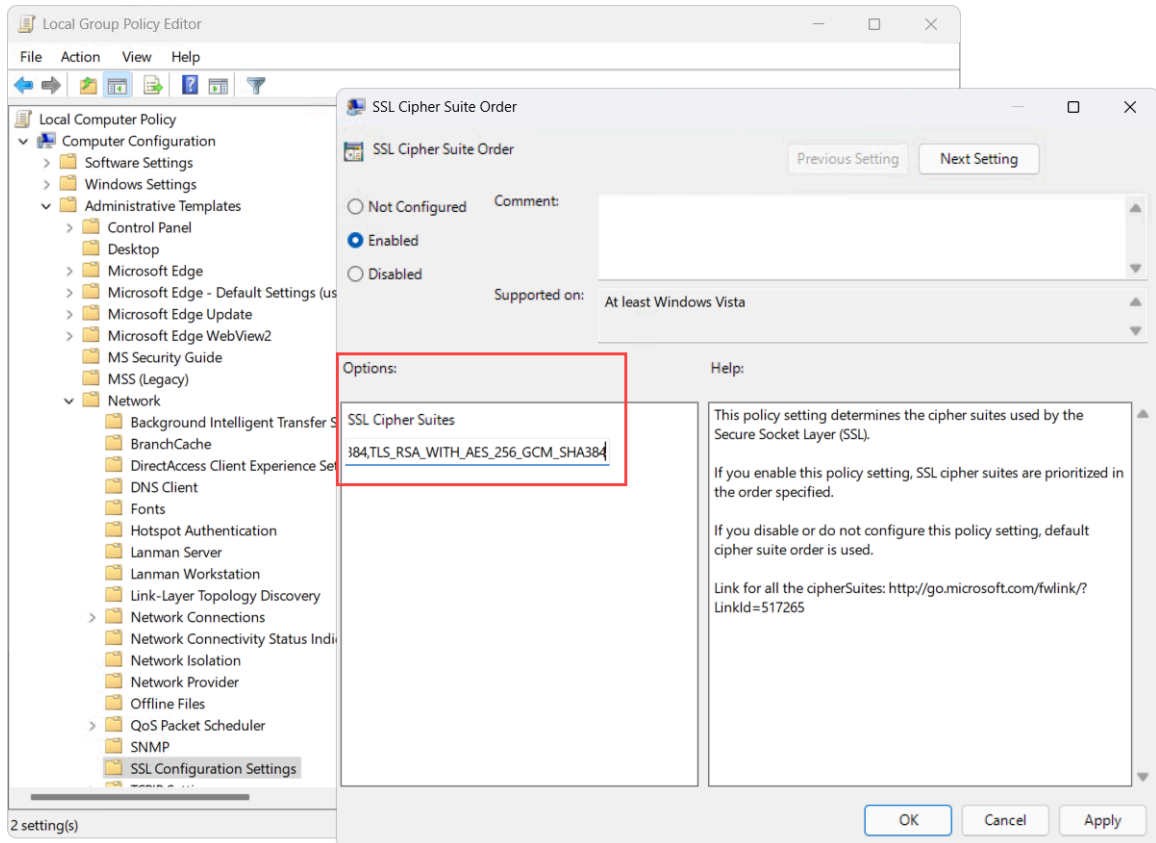
Según su integración, se debe agregar uno de los siguientes conjuntos de cifrado para permitir que las unidades se comuniquen con el dispositivo:

- **Integración del controlador Mercury LP en firmware 1.31 y anterior:**
 - TLS_RSA_WITH_AES_256_GCM_SHA384
 - TLS_RSA_WITH_AES_128_GCM_SHA256
- **Integración del controlador Mercury EP en firmware 1.29.7 y anterior:**
 - TLS_RSA_WITH_AES_256_CBC_SHA

Procedimiento

- 1 En Windows, ejecute `gpedit.msc` para abrir el *Editor de Políticas del Grupo Local*.
- 2 Vaya a **Configuración de la Computadora > Plantillas Administrativas > Red > Configuración de la Capa de Puertos Seguros (SSL, por sus siglas en inglés)**.
- 3 Haga doble clic en **Pedido del Conjunto de Cifrado de la Capa de Puertos Seguros (SSL, por sus siglas en inglés)**.
- 4 En el panel de *Opciones*, en el campo de **Conjuntos de Cifrado de la Capa de Puertos Seguros (SSL, por sus siglas en inglés)**, agregue una coma al final de la lista seguida del conjunto de cifrados aplicable a su integración. No agregue espacios.

- 5 Haga clic en **DE ACUERDO** para guardar el Objeto de Política de Grupo (GPO).



- 6 Reinicie el servicio Software o reinicie el dispositivo.

Habilitación del soporte para la integración de Synergis IX

Antes de poder inscribir controladores Synergis™ IX en su dispositivo Streamvault™, debe agregar un conjunto de cifrado Capa de Puertos Seguros (SSL, por sus siglas en inglés) adicional.

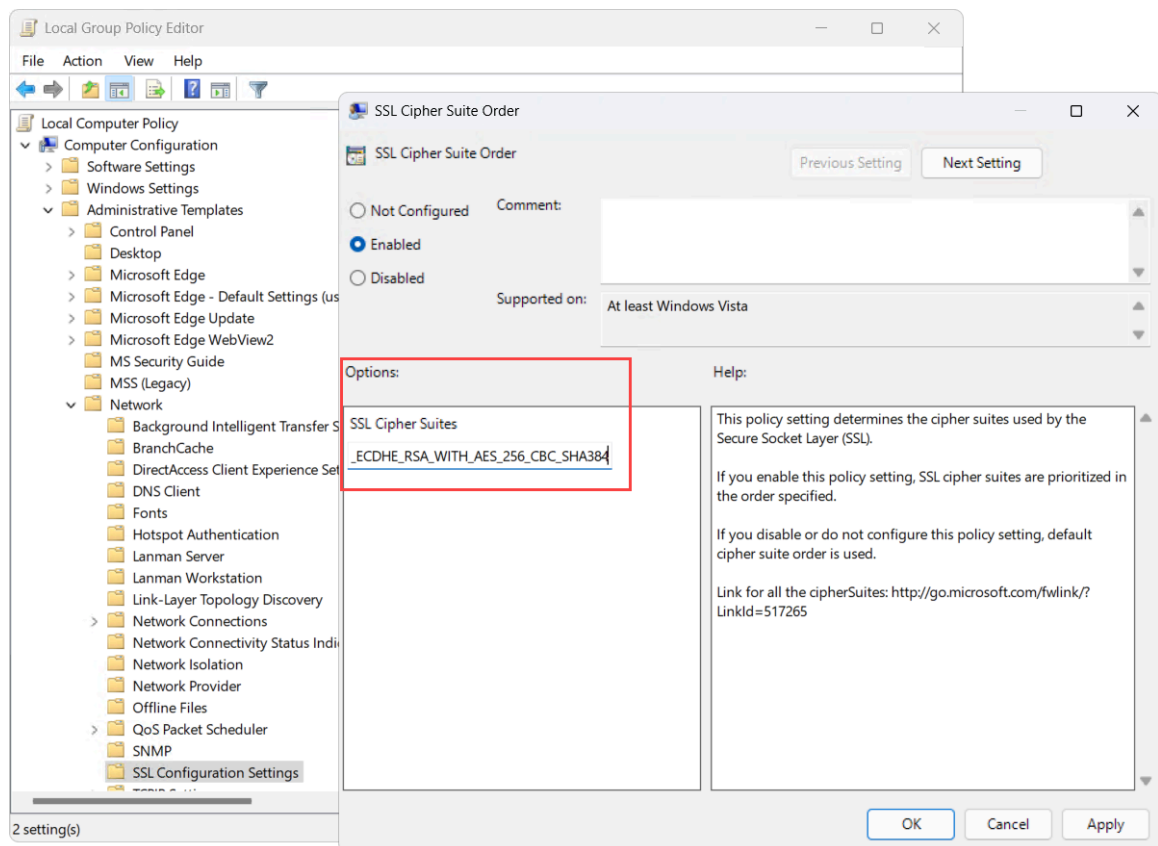
Lo que debería saber

Se debe agregar uno de los siguientes conjuntos de cifrado para inscribir los controladores Synergis IX en su dispositivo Streamvault:

- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256

Procedimiento

- 1 En Windows, ejecute `gpedit.msc` para abrir el *Editor de Políticas del Grupo Local*.
- 2 Vaya a **Configuración de la Computadora > Plantillas Administrativas > Red > Configuración de la Capa de Puertos Seguros (SSL, por sus siglas en inglés)**.
- 3 Haga doble clic en **Pedido del Conjunto de Cifrado de la Capa de Puertos Seguros (SSL, por sus siglas en inglés)**.
- 4 En el panel de *Opciones*, en el campo de **Conjuntos de Cifrado de la Capa de Puertos Seguros (SSL, por sus siglas en inglés)**, agregue una coma al final de la lista seguida de TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 o TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA256. No agregue espacios.
- 5 Haga clic en **DE ACUERDO** para guardar el Objeto de Política de Grupo (GPO).



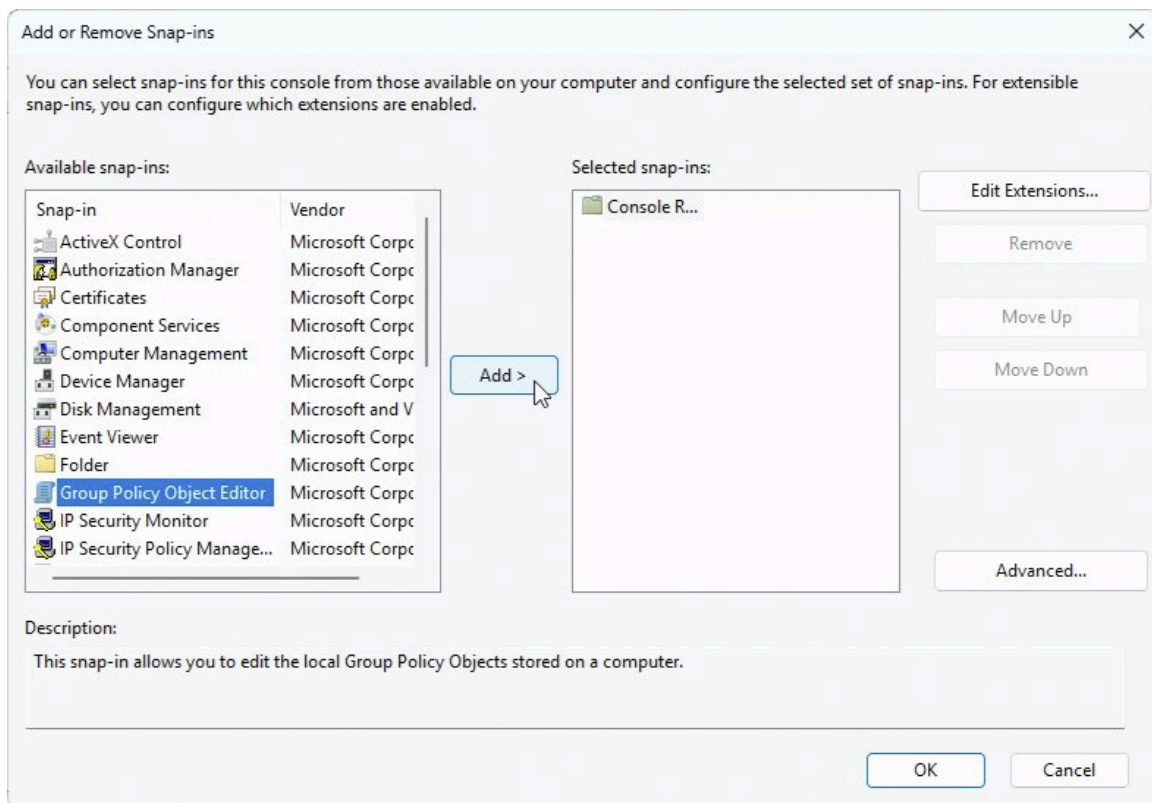
- 6 Reinicie el servicio Softwire o reinicie el dispositivo.

Modificación de GPO locales para cuentas de usuarios no administradores

De forma predeterminada, las cuentas de usuarios no administradores tienen acceso restringido a características del dispositivo Streamvault™. Para personalizar sus permisos, puede modificar los objetos de política de grupo local (GPO) para el grupo de **No administradores** mediante Microsoft Management Console.

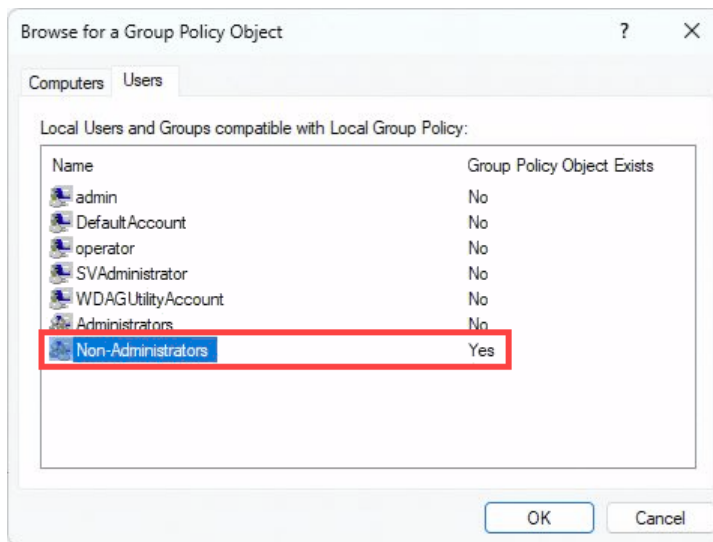
Procedimiento

- 1 Desde el menú de Inicio de Windows, seleccione **Ejecutar**. Luego escriba `mmc . exe` y haga clic en **Aceptar**. Se abre la ventana de *Microsoft Management Console*.
- 2 En el panel izquierdo, haga clic en **Archivo > Agregar o quitar complemento**. Se abre el cuadro de diálogo *Agregar o quitar complementos*.
- 3 En la sección **Complementos disponibles**, seleccione **Editor de objetos de política de grupos** y haga clic en **Agregar**.



- 4 En el asistente de *Objeto de política de grupos*, haga clic en **Buscar**.

- 5 En el cuadro de diálogo *Buscar un objeto de política de grupos*, haga clic en la pestaña **Usuarios**, seleccione el grupo de **No administradores** para el cual exista un GPO local y haga clic en **Aceptar**.

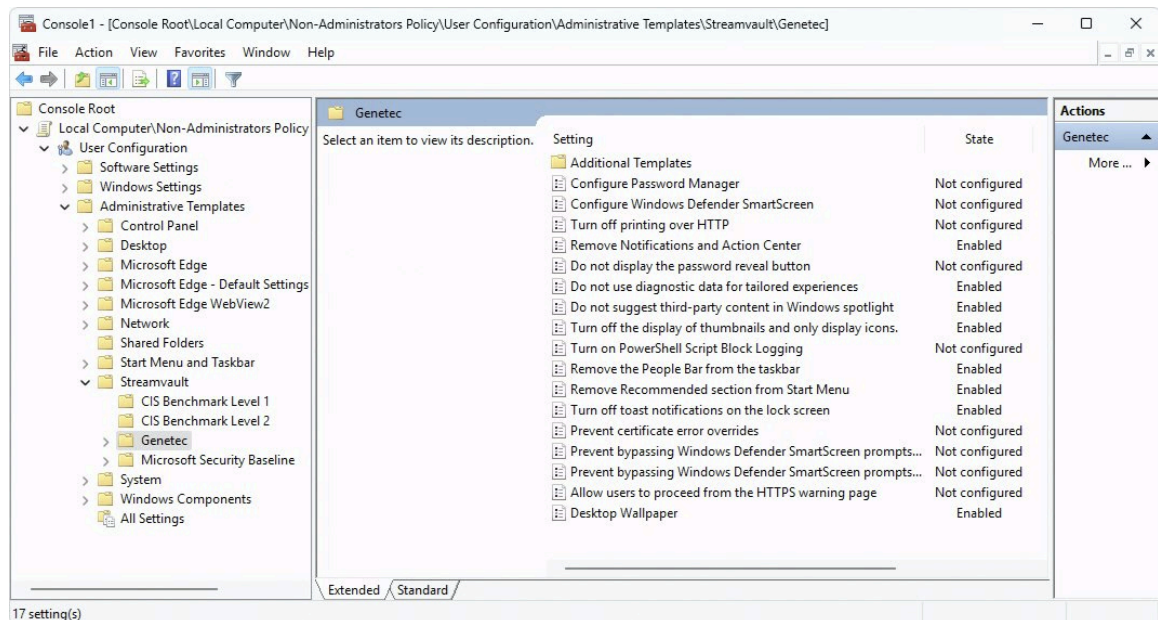


- 6 En el cuadro de diálogo *Seleccionar objeto de política de grupo*, haga clic en **Finalizar**.
- 7 En el cuadro de diálogo *Agregar o quitar complementos*, haga clic en **Aceptar**.
- 8 En la ventana *Microsoft Management Console*, vaya a **Raíz de consola > Computadora local/Política para no administradores > Configuración de usuarios > Plantillas administrativas > Streamvault > <perfil de endurecimiento>**,

donde <perfil de endurecimiento> representa uno de los cuatro perfiles de endurecimiento predefinidos: CIS Benchmark Level 1, CIS Benchmark Level 2, Genetec™ y Microsoft Security Baseline.

Todos los GPO que están configurados para cuentas de no administradores aparecen en el perfil de endurecimiento seleccionado.

NOTA: Un GPO está configurado si su estado es *Habilitado* o *Deshabilitado*. Un GPO con estado *No configurado* no es controlado por Streamvault.



- 9 Haga doble clic en los GPO individuales para verlos o editarlos.

Temas relacionados

[Información de inicio de sesión para las cuentas de usuario predeterminadas en un dispositivo Streamvault](#)
en la página 12

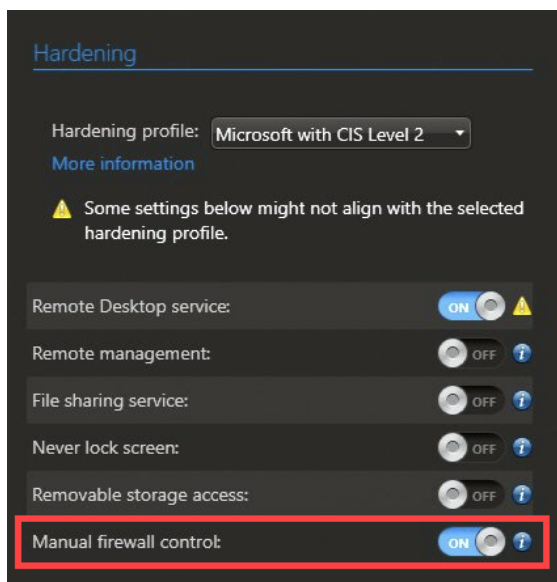
Cómo desactivar el firewall de Windows

De forma predeterminada, el firewall de Windows usa objetos de política de grupo local (GPO, por sus siglas en inglés) de los perfiles de endurecimiento para proteger el dispositivo Streamvault™. Si quiere desactivar el firewall de Windows para fines de solución de problemas, primero debe activar el control manual de firewall en SV Control Panel.

Procedimiento

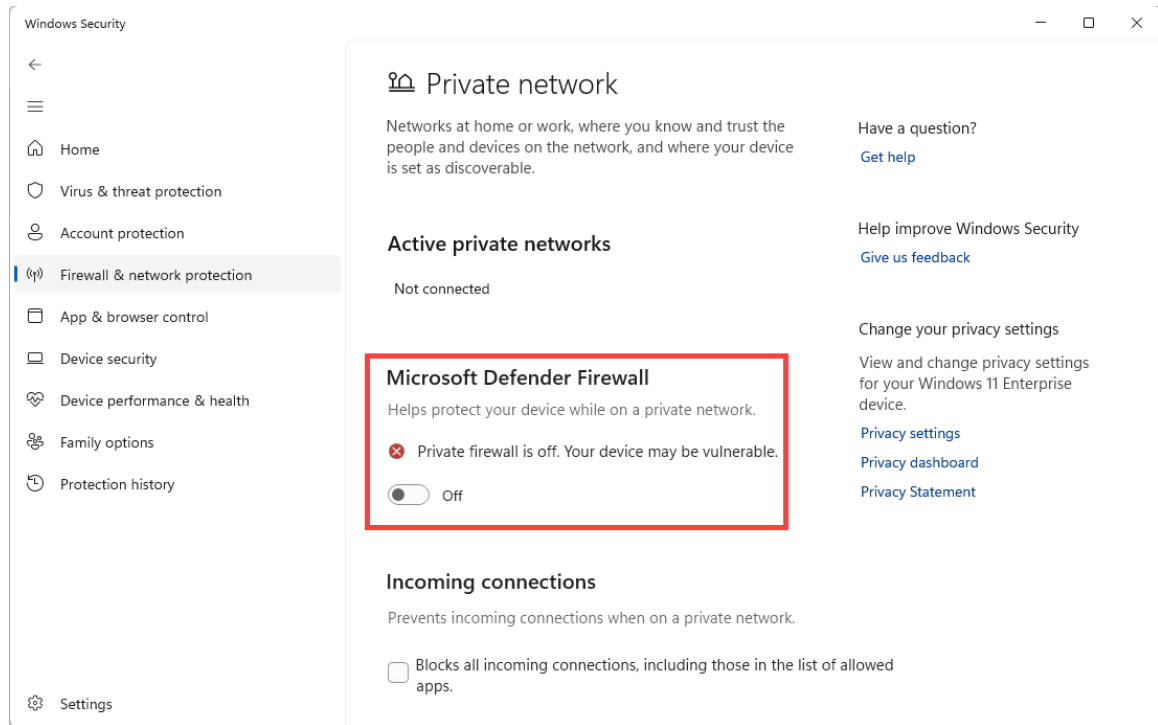
- 1 Abra SV Control Panel y vaya a la página *Seguridad*.
- 2 En la sección *Endurecimiento*, active la opción **Control manual de firewall** y haga clic en **Aplicar**. Espere que se apliquen los ajustes.

NOTA: Cuando esta opción está activada, todos los GPO locales están deshabilitados. Las reglas del firewall no se ven afectadas.



- 3 Desde el menú de inicio de Windows, abra **Firewall y protección de red**.
- 4 Seleccione la red cuyo firewall desee desactivar.

- 5 En la sección *Firewall de Microsoft Defender*, deshabilite el firewall.



NOTA: También puede deshabilitar el firewall mediante el *Firewall de Windows Defender con seguridad avanzada*.

Apoyo técnico

Esta sección incluye los temas siguientes:

- [" Comunicación con el Centro de Asistencia Técnica de Genetec "](#) en la página 129
- ["Soporte de software"](#) en la página 132
- ["Soporte de hardware"](#) en la página 133
- ["Especificaciones para Streamvault"](#) en la página 134
- ["Términos y condiciones del soporte de Streamvault"](#) en la página 135

Comunicación con el Centro de Asistencia Técnica de Genetec

El Centro de asistencia técnica de Genetec™ (GTAC) está disponible para ayudarlo con cualquier problema de software o hardware relacionado con Streamvault™.

NOTA: Para consultas sobre problemas del software Genetec™ Security Center, se ofrece asistencia técnica a través de nuestra línea regular de asistencia técnica. Para encontrar el número de teléfono de GTAC y el horario comercial en su región, consulte la página [Centro de Asistencia Técnica de Genetec Contacto](#).

Información útil

Al abrir un caso de soporte, tenga lista la siguiente información:

- Su ID del sistema de licencia de Security Center. Para obtener más información, consulte [¿Cómo encuentro la ID de mi sistema?](#).
- Su número de serie de Genetec o la etiqueta de servicio de hardware.
- Su código Genetec, que se encuentra en el chasis (no aplicable a dispositivos todo en uno). Necesitará el código si pierde el acceso administrativo al sistema y necesita una imagen de fábrica.



- Su archivo de registro de diagnóstico TSR (si corresponde). Para obtener más información, consulte [Recopilación de registros de soporte](#).

Contactar con GTAC por teléfono

La asistencia telefónica para problemas de Streamvault™ está disponible para todos los clientes durante el horario comercial de su región.

Para clientes de Norteamérica, Europa, Medio Oriente y África:

1. Consulte la página del [Portal de Asistencia Técnica de Genetec™ \(GTAC\) Contacto](#) para encontrar el número de teléfono de GTAC y el horario comercial de su región.
2. Llame al número de teléfono de GTAC y elija la Opción #2.

Para clientes de la región Asia-Pacífico:

El soporte para la región APAC se proporciona a través del [Portal de Asistencia Técnica de Genetec \(GTAP\)](#) a través del chat en vivo y los casos de soporte. El horario de atención es de lunes a viernes de 8 am a 8 pm (hora local).

Para el soporte de emergencia las 24 horas al día, 7 días a la semana fuera del horario comercial:

1. Llame al número GTAC de su región.
2. Introduzca su número de identificación de certificación de Genetec.
3. Ingrese el número de contrato de Genetec Advantage o el número de suscripción de Genetec.
4. Seleccione el producto.

- Deje un mensaje que incluya su nombre, número de teléfono y una descripción del problema.

El ingeniero de guardia se comunicará con usted en un plazo de 30 minutos.

IMPORTANTE: El soporte de emergencia 24 horas al día, 7 días a la semana está disponible solo para los clientes que hayan agregado esta opción a su contrato Genetec Advantage. Para más información, póngase en contacto con advantage@genetec.com.

Los clientes sin cobertura Advantage deben abrir un caso a través del [Portal de Asistencia Técnica de Genetec \(GTAP\)](#).

Contactando con el GTAC a través de GTAP

El soporte para los problemas de Streamvault™ está disponible para todos los clientes durante el horario comercial de su región a través de los casos de soporte en línea en el [Portal de asistencia técnica de Genetec™ \(GTAP\)](#).

Para los clientes sin cobertura Genetec™ Advantage, se debe abrir un caso a través de [Portal de Asistencia Técnica de Genetec \(GTAP\)](#). Para obtener más información sobre Genetec Advantage, comuníquese con ventaja@genetec.com.

Para enviar un caso a través del portal en línea:

- Navegue hasta el [Portal de Asistencia Técnica de Genetec](#).
- Inicie sesión con su correo electrónico corporativo.
- Haga clic en **+ Crear Caso**.



- Desde la lista **ID del sistema**, seleccione el sistema afectado.
- Para devolución o reparación de hardware, incluya **Solicitud de RMA** en el título para que nuestro equipo pueda identificar con facilidad estas solicitudes.

Description of the issue

Please Note:

- If you have more than one issue to report, please open one case for each
- If you have a problem with an order and/or its license parts, please contact customerservice@Genetec.com
- If you have any sales-related questions, please contact sales@Genetec.com
- If you are reporting a hardware issue with a StreamVault™ appliance, please type 'RMA' in the Title.

Title:

RMA Request [your title here]

Description:

[Your description here]

- Incluya el número de serie del producto, el código de Genetec y el archivo de registro TSR de diagnóstico (si corresponde).
- Hacer clic **Enviar caso**.

Recibirá una confirmación del caso por correo electrónico con el tiempo estimado de respuesta.

Contactando con el GTAC a través del chat en vivo

El soporte para los problemas de Streamvault™ está disponible para los clientes con cobertura Genetec™ Advantage a través del chat en vivo en el [Portal de Asistencia Técnica de Genetec \(GTAP\)](#). Los clientes pueden recibir soporte durante el horario comercial de su región.

Para los clientes sin cobertura Genetec Advantage, se debe abrir un caso a través de [Portal de Asistencia Técnica de Genetec \(GTAP\)](#). Para obtener más información sobre Genetec Advantage, comuníquese con advantage@genetec.com.

Para iniciar un chat en vivo:

1. Vaya al [Portal de Asistencia Técnica de Genetec](#)
2. Inicie sesión con su correo electrónico corporativo.
3. Haga clic en el botón **haga clic para chatear**.



4. Elija su idioma preferido.
5. Introduzca la ID completa del sistema (GSC-xxxxxx-xxxxxx), luego haga clic en **Verificar la ID del sistema**.
6. Elija si está chateando en relación a un caso nuevo o existente.
7. Seleccione el producto.
8. Haga clic en **Iniciar chat**.

A screenshot of the "GTAC - Live Chat" interface. At the top is a red header with the text "GTAC - Live Chat" and a dropdown arrow. Below the header, it says "Support hours for your territory: Monday to Friday: 08:00 to 20:00 Eastern Standard Time" and "Status: Online". The Genetec logo is displayed. The main content area is a white box with a "Welcome" message, a language selection section with radio buttons for "English" and "French", and a "Please enter the System ID" section with a text input field and a "CHECK SYSTEM ID" button. At the bottom of the white box, it says "The transcript of your chat session will be retained for quality assurance purposes" and a "START CHAT" button.

9. Para iniciar una RMA, incluya el número de serie del producto, el código de Genetec y el archivo de registro TSR de diagnóstico (si corresponde).

Tiempo de respuesta (disponible solo durante el horario comercial de su región): por lo general, en un plazo de 5 minutos.

Soporte de software

El software de imágenes Streamvault™ de Windows incluye la última versión del software Security Center y del panel de control en el momento de la creación de la imagen. La compatibilidad con la imagen de Windows y el software de Security Center se manejan por separado.

Software Streamvault

- La imagen de Windows de Streamvault está cubierta por la garantía de Streamvault durante todo el ciclo de vida del dispositivo.
IMPORTANTE: La actualización del sistema operativo Windows no está cubierta por la garantía. La actualización del sistema operativo Windows elimina los controladores, el refuerzo y el software necesarios instalados con la imagen.
- La imagen de respaldo proporcionada para la reimaginación de un dispositivo Streamvault incluye el sistema operativo original y la imagen proporcionada con el dispositivo al momento de la compra.
- La imagen de Windows de Streamvault está cubierta por su garantía de Streamvault de forma independiente de su estado de Genetec™ Advantage.

Software del centro de seguridad

Los problemas con el software Security Center están cubiertos por el acuerdo de nivel de servicio (SLA, por sus siglas en inglés) y los procedimientos de soporte descritos en el documento de Genetec™ Lifecycle Management (GLM): [Descripción de Genetec Advantage](#).

Soporte de hardware

HP y [Soporte profesional de Dell](#) Las garantías están disponibles a través de Genetec™. Para cualquier problema de hardware, el Centro de asistencia técnica de Genetec™ (GTAC) es su punto de contacto para diagnosticar el problema y coordinarlo con HP y Dell ProSupport.

Consulte la [Descripción General de la Garantía de Hardware de Genetec](#) para obtener detalles sobre las garantías de hardware de Streamvault que ofrece Genetec.

Especificaciones para Streamvault

Cuando planifique e implemente el dispositivo de Streamvault™, tenga en cuenta las siguientes especificaciones técnicas, mecánicas y ambientales.

Especificaciones técnicas, mecánicas y ambientales.

Dispositivos todo en uno:

- [Hoja de datos del SV-300E](#)

Dispositivos para montaje en rack:

- [Hoja de datos de la serie SV-1000E](#)
- [Hoja de datos de la serie SV-2000E](#)
- [Hoja de datos de la serie SV-4000E](#)

Almacenamiento centralizado de alta disponibilidad:

- [Hoja de datos de la serie SV-7000EX](#)

Estaciones de trabajo:

- [Ficha técnica de la serie SVW-100E](#)
- [Hoja de datos de la serie SVW-300E](#)
- [Hoja de datos de la serie SVW-500E](#)

Dispositivos de Vehicle Monitoring todo en uno:

- [Hoja de datos de la serie SVR-300A](#)
- [Hoja de datos de la serie SVR-300AR](#)
- [Hoja de datos de la serie SVR-500A](#)

Términos y condiciones del soporte de Streamvault

Las garantías de hardware Estándar y Extendidas de Genetec™ se rigen por los términos y condiciones descritos en [Descripción General de la Garantía de Hardware de Genetec](#).

Glosario

Administrador de Streamvault™

La entidad Streamvault™ Manager se usa para controlar las configuraciones de alertas para un grupo de entidades de Streamvault™ Agent. Solo se permite un administrador Streamvault™ por sistema.

dispositivo SV

Streamvault™ es un dispositivo llave en mano que viene con un sistema operativo integrado y Security Center preinstalado. Puede utilizar dispositivos Streamvault™ para implementar de manera rápida un sistema de videovigilancia y control de acceso unificado o autónomo.

Hardware de Streamvault™:

El hardware Streamvault™ es una tarea de informe en Security Center que puede usar para ver una lista de problemas de salud que afectan sus dispositivos Streamvault™.

imagen de fabricación

Una imagen de fabricación es una imagen de Streamvault™ que se envía a los clientes cuando compran un dispositivo. Las versiones de software instaladas en esta imagen varían según el pedido del cliente.

imagen de recuperación

Se usa una imagen de recuperación para volver a crear la imagen de los dispositivos Streamvault™. Es una imagen fija con versiones de software específicas preinstaladas.

Monitor de hardware de Streamvault™

La entidad de monitor de Hardware de Streamvault™ se usa para monitorear el estado de sus dispositivos Streamvault™ y garantizar que reciba notificaciones cuando ocurran problemas. Se requiere un monitor de hardware Streamvault™ por dispositivo Streamvault™.

Servicio Streamvault

El servicio Streamvault es un servicio de Windows que permite a los usuarios configurar un dispositivo Streamvault™, como por ejemplo aplicar perfiles de endurecimiento.

SV-1000E

El SV-1000E es un dispositivo de seguridad montado en bastidor rentable diseñado para sistemas de seguridad de tamaño intermedio. Le permite pasar a un sistema de seguridad unificado que combina videovigilancia, control de acceso, reconocimiento automático de placas de matrícula, comunicaciones, detección de intrusión y analíticas en un solo dispositivo. El SV-1000E viene con Security Center y el Panel de control SV preinstalados.

SV-100E

SV-100E es un dispositivo subcompacto y todo en uno que viene con Microsoft Windows, Security Center y SV Control Panel preinstalados. SV-100E es para instalaciones de servidor único a pequeña escala, y es compatible con cámaras y lectores de control de acceso.

SV-2000E

SV-2000E es un dispositivo de seguridad de montaje en bastidor que le permite implementar de manera simple un sistema unificado que combina videovigilancia, control de acceso, reconocimiento automático de placas vehiculares y comunicaciones. El SV-2000E viene con Security Center y el Panel de control SV preinstalados.

SV-300E

SV-300E es un dispositivo compacto de llave en mano y todo en uno que viene con Microsoft Windows, Security Center y SV Control Panel preinstalados. Con las tarjetas de captura de codificador analógico integradas, puede usar el dispositivo para implementar de forma rápida un sistema de control de acceso o videovigilancia independiente, o un sistema unificado.

SV-350E

SV-350E es un dispositivo de seguridad todo en uno y llave en mano que le permite pasar a un sistema de seguridad unificado que combina videovigilancia, control de acceso, detección de intrusión y comunicaciones. Viene con Microsoft Windows, Security Center y SV Control Panel preinstalados. Ofrece RAID 5 para almacenamiento de video crítico.

SV-4000E

SV-4000E es un dispositivo de seguridad de montaje en bastidor que ofrece rendimiento y confiabilidad de grado empresarial. Sus configuraciones de hardware certificadas y su refuerzo listo para usar contra amenazas cibernéticas simplifican el diseño y la implementación de un nuevo sistema de seguridad. El SV-4000E viene con Security Center y el Panel de control SV preinstalados.

SV-7000E

SV-7000E es un dispositivo de seguridad de montaje en bastidor diseñado para aplicaciones que combinan una gran cantidad de cámaras de alta resolución, usuarios y eventos. El SV-7000E viene con Security Center y el Panel de control SV preinstalados.

SVA-100E

SVA-100E es un dispositivo compacto que puede utilizar para mejorar de manera fácil su sistema de seguridad con KiwiVision™ video analytics. El diseño está optimizado para que pueda aplicar más flujos de análisis a su sistema de videovigilancia, ya sea un flujo analítico único o múltiple, por cámara.

SV Control Panel

SV Control Panel es una aplicación de interfaz de usuario que puede utilizar para configurar su dispositivo Streamvault™ para que funcione con el control de acceso y la videovigilancia de Security Center.

SVW-300E

La estación de trabajo de SVW-300E es una solución llave en mano diseñada para monitorear sistemas de seguridad de tamaño pequeño y mediano con soporte para múltiples pantallas. El SVW-300E viene con Security Center preinstalado.

SVW-500E

La estación de trabajo SVW-500E es una solución de alto rendimiento diseñada para usuarios que necesitan la capacidad de ver cámaras con una resolución muy alta en monitores 4K y paredes de video. El SVW-500E viene con Security Center preinstalado.

Utilidad de restablecimiento de fábrica de Streamvault

La utilidad de restablecimiento de fábrica de Streamvault es una herramienta que le permite restablecer un dispositivo Streamvault a sus valores de fábrica. Esta herramienta lo ayuda a crear una memoria USB de arranque con la imagen del software de Streamvault necesaria.

Dónde encontrar información del producto

Puede encontrar la documentación de nuestro producto en las siguientes ubicaciones:

- **Genetec™ TechDoc Hub:** La documentación más reciente está disponible en [TechDoc Hub](#).
¿No puede encontrar lo que anda buscando? Póngase en contacto con documentation@genetec.com.
- **Paquete de instalación:** La Guía de Instalación y las Notas de la Versión están disponibles en la carpeta Documentación del paquete de instalación. Estos documentos también tienen un enlace de descarga directa a la última versión del documento.
- **Ayuda:** Las aplicaciones de Security Center de cliente y basadas en la web incluyen ayudas que explican cómo funciona el producto y proporcionan instrucciones sobre cómo usar las características del producto. Para tener acceso a la ayuda, haga clic en **Ayuda**, presione F1 o toque la tecla ? (signo de interrogación) en las diferentes aplicaciones cliente.