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: 16 de noviembre de 2023

Avisos legales

©2023 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 cualquier persona o entidad con respecto a cualquier pérdida o daño que sea incidental o consecuencial de las instrucciones que se encuentran en este documento o los productos de software y hardware de computadora descritos en este documento.

Genetec™, AutoVu™, AutoVu MLC™, Citywise™, Community Connect, Curb Sense™, Federation™, Flexreader™, Genetec Airport Sense™, Genetec Citigraf™, Genetec Clearance™, Genetec ClearID™, Genetec Mission Control™, Genetec Motoscan™, Genetec Patroller™, Genetec Retail Sense™, Genetec Traffic Sense™, KiwiVision™, KiwiSecurity™, Omnicast™, Privacy Protector™, Sipelia™, Stratocast™, Streamvault™, 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, Citigraf, 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: 16 de noviembre de 2023

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 Panel de control de SV. 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

Capítulo 4: Referencia de SV Control Panel

Capítulo 5: Recursos adicionales

Capítulo 6: Solución de problemas

Capítulo 7: Soporte técnico

1

Introducción a su dispositivo Streamvault

Esta sección incluye los temas siguientes:

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 puede 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.	• Puertos predeterminados utilizados por Streamvault en la página 4. • Conectar los componentes del dispositivo Streamvault en la página 8. • Tarjetas codificadora analógica 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, lea las notas de la versión para conocer las nuevas funciones, los problemas conocidos y las limitaciones.	En las *Notas de la versión de Streamvault* correspondientes a la versión de imagen instalada en su dispositivo, consulte: • Qué hay de nuevo • Problemas conocidos • Limitaciones
3	Inicie sesión en Windows como Administrador con la contraseña que está impresa en su dispositivo y, luego, cambie la contraseña.	• Iniciar sesión en un Streamvault aparato en la página 12.
Complete los asistentes de configuración		
4	Complete el asistente de *configuración de Streamvault Control Panel*. **NOTA:** El escritorio remoto está deshabilitado de manera predeterminada. Para habilitar el escritorio remoto, desactive la configuración de **Bloquear escritorio remoto** en la página de *Seguridad* de este asistente.	• Configuración de su dispositivo en SV Control Panel en la página 15. • Permitir conexiones a Escritorio Remoto con un dispositivo Streamvault en la página 72.
5	Active su licencia de Security Center. • Si el dispositivo está conectado a internet, active su licencia mediante el asistente de *Activación del Panel de Control de Streamvault.* • Si el dispositivo no está conectado a internet, active su licencia de forma manual desde Server Admin.	• Activar su licencia de Security Center en un dispositivo en la página 18. • Activar una licencia de manera manual desde Server Admin en la página 20.

Paso	Tarea	Dónde puede encontrar más información
6	Active System Availability Monitor.	• Activar System Availability Monitor en la página 22.
7	Configure Genetec™ Update Service para poder obtener la última versión de Security Center y SV Control Panel. Si hay actualizaciones, instálelas.	• En la *Guía del Usuario de Genetec™ Update Service*, consulte "Configurar Genetec Update Service".
8	Si SV Control Panel indica que hay más actualizaciones disponibles, instálelas ahora.	• Acerca de la actualización del software de SV en la página 7.
9	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.	• Para las series SV-1000E, SV-2000E, SV-4000E: Añadir funciones de Archiver en SV Control Panel en la página 36. • Para SV-7000E y para dispositivos Todo en uno: Adición manual de particiones y roles de Archiver en la página 38.
10	Inicie sesión en Config Tool y configure sus características de video y control de acceso de Security Center.	• Habilitar las funciones de control de acceso y video de Security Center en la página 23. • Configurar los ajustes de inscripción de la unidad en la página 26.
11	Realice una copia de respaldo de la configuración de Security Center.	• Crear una copia de respaldo de la base de datos de su Directory en la página 33.

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 plugin Streamvault™ Maintenance

La siguiente tabla enumera los puertos que deben abrirse para el tráfico entrante para que el plugin Streamvault™ Maintenance pueda comunicarse con el hardware de Streamvault.

Módulo	Puerto entrante	Uso del puerto
Monitor de hardware de Streamvault	65115	Se utiliza para comunicarse 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 Panel de Control de StreamVault

La siguiente tabla enumera los puertos que deben abrirse para el tráfico saliente para que los componentes del Panel de Control de Streamvault puedan conectarse 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

La siguiente tabla enumera los puertos que deben abrirse para el tráfico saliente para que el agente de escritorio CylancePROTECT pueda comunicarse con la consola de administración de Genetec y recibir actualizaciones del agente.

Puerto de salida	Uso del puerto	URL de destino
TCP 443	Comunicación HTTPS en América del Norte	cemento.cylance.com datos.cylance.com proteger.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

Puerto de salida	Uso del puerto	URL de destino
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 venueapi.us.cylance.com

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

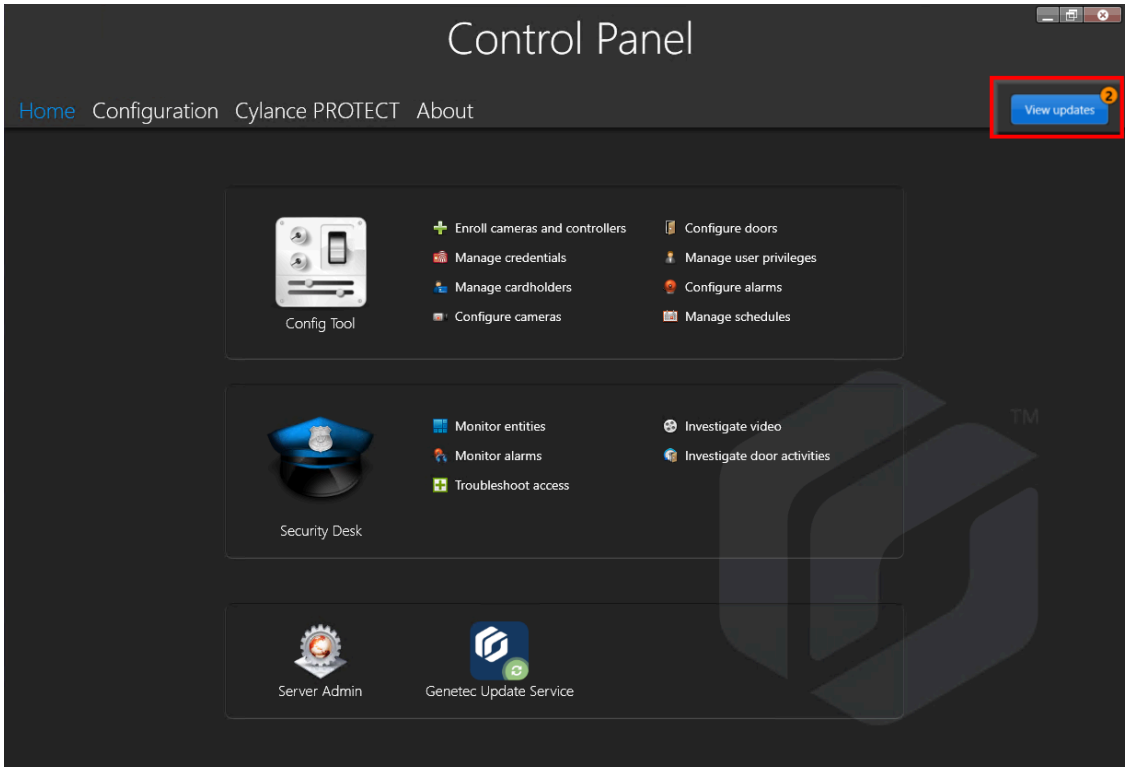
Para obtener más información sobre los modos en los que el dispositivo Streamvault se comunica con los servicios de administración de Genetec, consulte Página de CylancePROTECT de SV Control Panel en la página 62.

Acerca de la actualización del software de SV

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

Cuando hay 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 consultó las actualizaciones por última vez.
- Actualiza automáticamente la licencia en segundo plano para garantizar que sea válida y que se actualice la fecha de vencimiento.
- Habilite diversas características, como el Programa de Mejora de Genetec.
- Revisa su firmware y recomienda actualizaciones o le notifica sobre vulnerabilidades.

Para obtener más información acerca de cómo usar GUS, consulte la *Guía del usuario de Genetec™ Update Service*.

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

Despeje el espacio alrededor del botón de encendido. Para evitar el apagado accidental del dispositivo, asegúrese de que nada toque o esté demasiado cerca del botón de encendido.

Para conectar los periféricos y la alimentación al dispositivo:

1 Conecte el cable del monitor de pantalla a una entrada de video compatible: VGA, HDMI o conector DisplayPort.

Debe conectar al menos un monitor 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 y, luego, conecte el otro extremo del cable al conector RJ-45 de la red IP.

6 Para los electrodomésticos 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, y luego enchufe el cable del bloque a un tomacorriente.

7 Para encender el dispositivo Streamvault, pulse el botón de encendido.

Después de que concluya

Inicie sesión en su dispositivo Streamvault.

Tarjetas codificadora analógica de Genetec

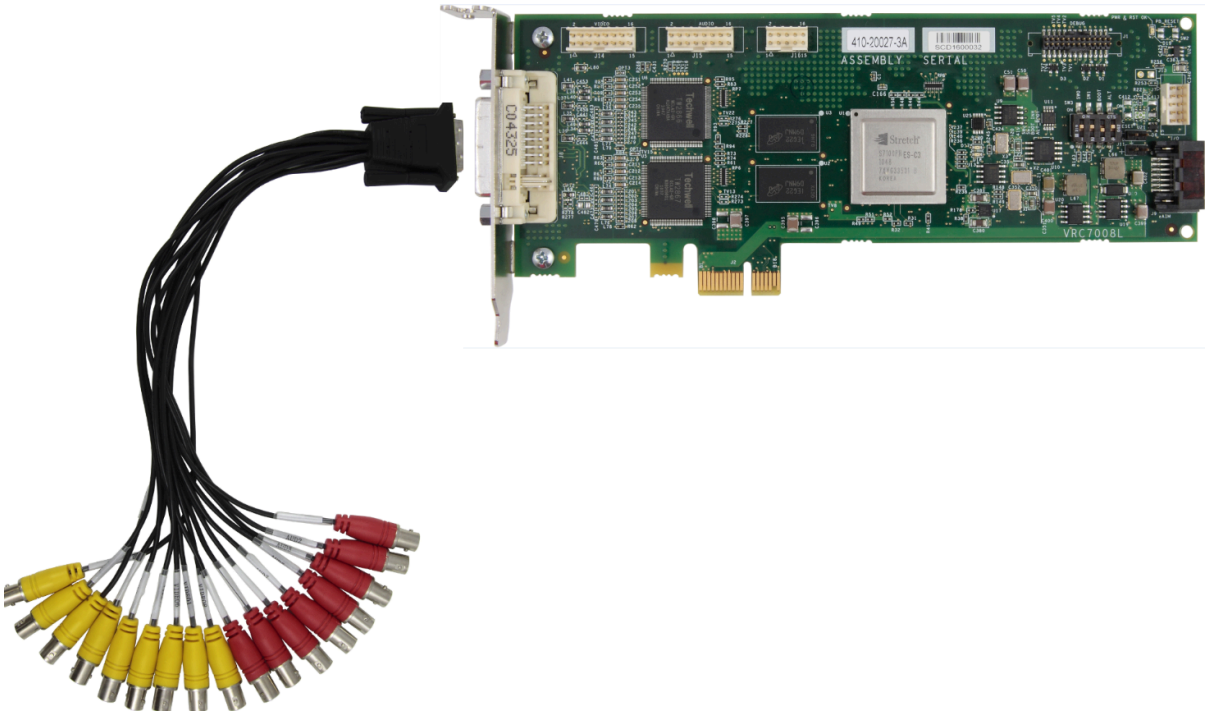
Si está utilizando un dispositivo Streamvault para implementar un sistema de videovigilancia con cámaras analógicas, debe conectarlas a la tarjeta codificadora analógica de Genetec™ en el dispositivo.

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 video máx. 4CIF
- Velocidad de cuadros máxima: 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, se la envía con un cable de conexión con conectores BNC para conectar las cámaras analógicas de manera directa a la tarjeta codificadora integrada.

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 acerca de la Herramienta de inscripción de la unidad, consulte la *Guía del Administrador de Security Center*.

Tenga en cuenta lo siguiente al agregar cámaras analógicas:

- No puede agregar cámaras analógicas en Security Center mediante el método de *Agregado manual*. Debe utilizar la herramienta de inscripción de unidades.
- Para descubrir nuevas unidades y utilizar la Herramienta de inscripción de la unidad, debe conectarse a Config Tool de forma local.
- Al seleccionar el fabricante de la cámara en la Herramienta de inscripción de la unidad, todas las cámaras analógicas figuran en la sección de *Tarjeta codificadora de 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.

Para deshabilitar las entradas de cámara en tarjetas codificadoras:

1 Desde la página de inicio de Config Tool, haga clic en la pestaña de *Acerca de*.

2 Haga clic en la pestaña de **Omnicast**™ y verifique la cantidad de cámaras que aparece 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 múltiples cámaras presionando Ctrl y haciendo clic en las cámaras.

6 En la parte inferior de la página de *Periféricos*, haga clic en el círculo rojo ( ) para deshabilitar las cámaras y luego haga clic en **Aplicar**.
Las páginas 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, y podrá ver reproducción desde esa cámara.

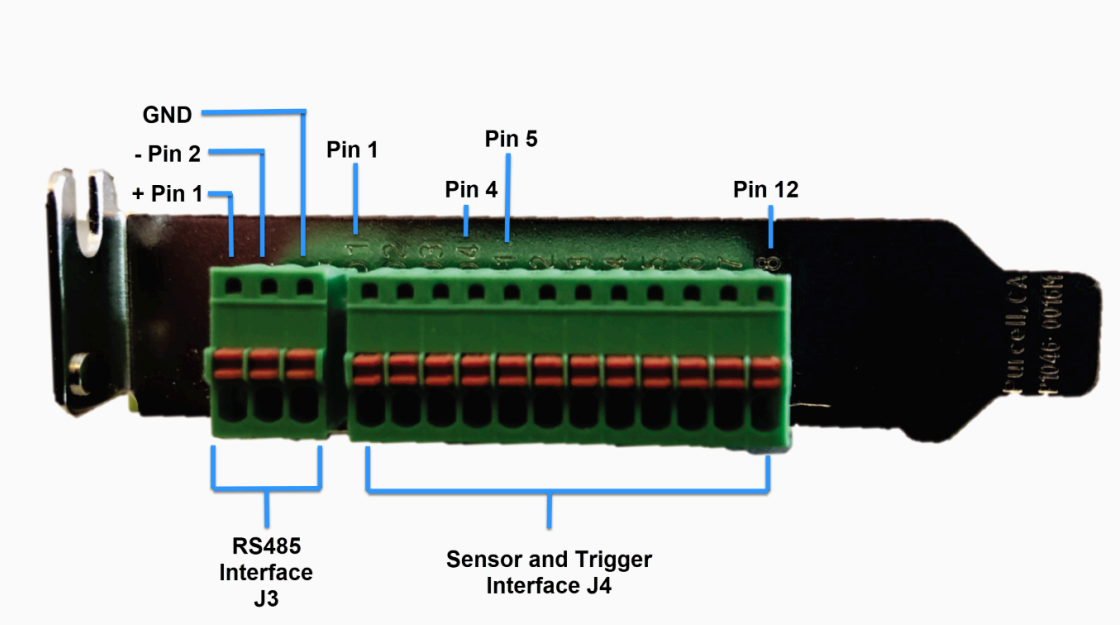
Entradas y salidas de alarma de un Streamvault aparato

Si está utilizando un dispositivo Streamvault para implementar un sistema de control de acceso, puede utilizar la tarjeta de E/S para conectar entradas de alarma de hardware de manera directa al dispositivo, y luego controlar sus salidas utilizando 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 conectar entradas de E/S

Si pide el dispositivo Streamvault con tarjeta 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 dispositivo. Los cables deben insertarse utilizando un destornillador plano pequeño para introducir las abrazaderas a presión en el conector.

Acerca de la creación de eventos a acciones

Para obtener información sobre cómo crear eventos a toma de acción para las entradas y salidas del dispositivo Streamvault, consulte la *Guía del Administrador de Security Center*.

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 debe cambiar 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

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

IMPORTANTE: Las contraseñas deben cumplir con los siguientes requisitos:

- Deben tener 10 caracteres como mínimo
- 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 $, %, !)

Para iniciar sesión en su dispositivo Streamvault por primera vez:

1. Encienda el dispositivo.
2. Inicie sesión con el nombre de usuario del Administrador y la contraseña predeterminada que están impresos en el dispositivo.
3. Introduzca 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. Introduzca una nueva contraseña de Operador.

   Ha iniciado sesión como un usuario Operador.
6. Continúe con la sesión del Operador o cierre sesión y vuelva a iniciar sesión como un usuario Administrador.

Después de que concluya

Inicie la configuración inicial de su dispositivo.

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. Server Admin 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: • Windows: todas las funciones administrativas y del sistema • Security Center • SV Control Panel	No aplica
Operador	operador	• Papelera de reciclaje • Bibliotecas • Mi PC • C: conducir • Página de inicio de SV Control Panel, solo configuración Regional de la página de Configuración, página de Acerca de • Server Admin: requiere contraseña de Administrador para los derechos completos	• Windows: apagar y reiniciar • Configuración del sistema • Partición de video
No aplica	genetecfactory	Administrador del servidor	No aplicable hasta que se complete SV Control Panel. **NOTA:** Esta opción no está disponible para dispositivos Workstation.

Para cambiar las contraseñas para 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. Sobre el *Configuración* página, en la *Configuración de la cuenta de usuario* sección, puede administrar todas sus contraseñas.

NOTA: La cuenta del Operador no se crea con una plantilla. Si crea una nueva cuenta de usuario, no tendrán las mismas restricciones por defecto.

Server Admin de Security Center

- Solo los usuarios Administradores pueden iniciar sesión en Server Admin.
- Para iniciar sesión desde su máquina local, haga clic en el acceso directo de **Server Admin** en su escritorio.
- Para iniciar sesión en Server Admin desde una máquina 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.

2

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 de 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.

PRECAUCIÓN: Los cambios de configuración realizados en SV Control Panel sobrescriben los cambios de configuración realizados fuera de 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 de directorio para configuraciones que se ejecutan en el servidor principal.

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.
- La opción para habilitar y deshabilitar Genetec™ Mobile y Synergis™ Softwire desde la sección de *Características* de la página de *Configuración*, si están instalados en el dispositivo.
- Enlaces a GTAP y documentación del producto.
- Página de configuración de comunicación con CylancePROTECT para elegir el modo en el que su dispositivo Streamvault™ se comunica con la Consola en la nube.
- La capacidad de crear funciones y particiones adicionales de Archiver para configuraciones en servidores de expansión.

NOTA: Guía aplicable para Streamvault Control Panel versión 2.8 y anteriores.

Configuración de su dispositivo en SV Control Panel

La primera vez que inicia sesión en su dispositivo Streamvault™, SV Control Panel abre el asistente de *configuración de Streamvault Control Panel* 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 un Archiver, Analíticas, Estación de Trabajo o cualquier otro dispositivo que sea un servidor de expansión de Security Center, no se le solicitará que cambie ninguna contraseña de usuario.

Para configurar su electrodoméstico:

1 Ponga en marcha 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. En los reinicios posteriores, los usuarios deben iniciar sesión con sus credenciales de Administrador e iniciar 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) Para un dispositivo con dos tarjetas de interfaz de red, seleccione la tarjeta que desea configurar desde la lista de **Interfaz de red**.

La lista de **Interfaces de red** está oculta cuando solo se conecta una tarjeta de interfaz de red.

b) Si usa DHCP para obtener una IP de manera automática (predeterminado) y falta la dirección IP, haga clic en **Actualizar** ( ) para obtener una nueva dirección IP y luego haga clic en **Reintentar**.

c) Si desea especificar la configuración de IP, haga clic en **Usar configuración estática**, e introduzca una dirección IP única para este dispositivo.

d) Si el campo **Estado** muestra algo diferente a "Conectado a Internet", haga clic en **Reintentar**.

e) Cuando el campo **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 SV Control Panel.

c) Cuando se vuelva a abrir el asistente de *configuración del Streamvault Control Panel*, en la página de *Configuración del equipo*, haga clic en **Siguiente**.

6 Sobre el *Seguridad* página, cambio la contraseña que ingresa el usuario administrador para iniciar sesión en Windows.

De manera predeterminada, esta contraseña también se usa para iniciar sesión en todas las aplicaciones de Genetec™. No se le solicita que cambie ninguna contraseña en un dispositivo que sea un servidor de expansión de Security Center.

7 En el **Seguridad** sección, configure las contraseñas haciendo clic en **Modificar la contraseña** para las siguientes aplicaciones:

- **Administrador de Windows:** La contraseña del usuario administrador para Windows.
- **aplicaciones cliente:** 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.

8 Configure los siguientes ajustes de seguridad y, luego, haga clic en **Siguiente**:

- **Cierre de sesión automático:** Active esta opción para configurar Windows para que cierre la sesión de un usuario después de 15 minutos de inactividad.
- **Complejidad de la contraseña:** Active esta opción para solicitar una contraseña compleja de al menos 10 caracteres para los usuarios de Windows.
- **Funciones de gestión del servidor:** Active esta opción para permitir funciones como agregar funciones y otras tareas con aplicaciones como *Windows Admin Center*, *Server Manager* o *Windows PowerShell*.
- **Acceso de almacenamiento que se puede eliminar:** Active esta opción para habilitar el acceso a una memoria USB o un disco duro USB conectado desde Windows.

  NOTA: Los usuarios con privilegios administrativos tienen acceso al almacenamiento extraíble de forma automática.
- **Habilitar compatibilidad con las tarjetas inteligentes:** Active esta opción para crear o utilizar un lector de tarjetas inteligentes con la aplicación Security Desk. Para evitar que el software malintencionado afecte al dispositivo, esta opción se ha desactivado de forma predeterminada.
- **Conexiones remotas entrantes:** Active esta opción para permitir el acceso a las conexiones de *Escritorio Remoto* y la función de compartir archivos al dispositivo desde su red de computadoras. Para

evitar que el software malintencionado afecte al dispositivo, esta opción se ha desactivado de forma predeterminada.

- **Escritorio Remoto:** Active esta opción para permitir que las personas de su red inicien sesión en el dispositivo mediante una aplicación de *Escritorio Remoto*. La opción de **Conexiones remotas entrantes** también debe estar habilitada para permitir el acceso al *Escritorio Remoto*. Para evitar que el software malintencionado afecte al dispositivo, esta opción se ha desactivado de forma predeterminada.
- **Uso compartido de archivos:** Active esta opción para compartir archivos y carpetas que se encuentran en el dispositivo con personas en su red. La opción de **Conexiones remotas entrantes** también debe estar habilitada para permitir el uso compartido de archivos. Para evitar que el software malintencionado afecte al dispositivo, esta opción se ha desactivado de forma predeterminada.

9 Lea la información en la página de *Acerca de CylancePROTECT* y haga clic en **Siguiente**.

10 En la página para *Configurar CylancePROTECT*, 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.

IMPORTANTE: Cuando CylancePROTECT está desactivado, no se puede cambiar entre **Desconectado** y **En línea**. Para cambiar esta configuración, debe restablecer la imagen del software en su dispositivo.

11 Para tener acceso a los registros y las características avanzadas de su sistema, seleccione la opción de **Ejecutar CylancePROTECT en Modo de IU Avanzado**.

12 Haga clic en **Siguiente**.

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

- **No recopilar datos:** 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 salud se envían a un Servicio de Monitoreo de Salud dedicado donde los nombres de las entidades están disfrazados y no se puede rastrear. Genetec Inc. usa estos datos solo para fines estadísticos y no es posible tener acceso a ellos a través del 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.

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

15 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 la desmarca, aparecerá un recordatorio para activar el producto en otro momento.

NOTA: Su dispositivo debe activarse antes del uso.

Después de que concluya

Active su dispositivo.

Activar su licencia de Security Center en un dispositivo

El asistente de *activación de Streamvault Control Panel* le ayuda a activar su licencia de Security Center en su dispositivo Streamvault™.

Antes de empezar

- Conecte su dispositivo 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 debe activar la licencia de Security Center en el dispositivo que aloja la función del Directory, no en dispositivos que sean servidores de expansión o estaciones de trabajo.

Para activar su licencia de Security Center mediante el ID del Sistema:

1 Desde SV Control Panel, 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 recibe el mensaje Se requiere acceso a Internet para la activación, el dispositivo no está conectado a Internet en este momento. Conecte su dispositivo ahora o active su licencia de forma 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 actualizaciones falla porque el Directory no responde, haga clic en **Abrir Server Admin** y asegúrese de que el Directory esté listo.

NOTA: Si Genetec Update Service no estaba listo en ese momento, la verificación de actualizaciones podría mostrar un error con el mensaje *No es posible verificar las actualizaciones en este momento. Lo intentaremos de nuevo más tarde.*

7 En la página de *Características adicionales*, habilite o deshabilite Synergis™ Softwire 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 Server Admin en la página 20
Acerca de la página de SV Control Panel en la página 63
Información de licencia en la página 63

Activar una licencia de manera manual desde Server Admin

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

Para activar una licencia de manera manual desde Server Admin:

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**.

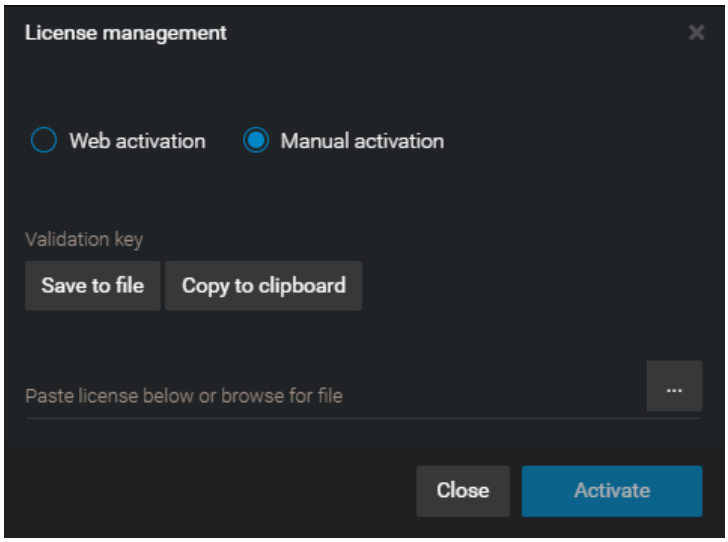
c) Inicie sesión en Administrador del servidor.

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 del archivo es *validation.vk*.



f) Copie el archivo *validation.vk* en una memoria USB.

g) Ejecute la memoria USB desde la computadora.

2 Obtenga la licencia desde el GTAP:
   a) En otra computadora con acceso a Internet, conecte la memoria USB.
   b) Inicie sesión en el 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) En la página de *Información del sistema*, en la sección de *Información de la licencia*, haga clic en **Activar 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

Activar su licencia de Security Center en un dispositivo en la página 18

Activar System Availability Monitor

Para monitorear los problemas de disponibilidad y de estado de salud de su sistema en el GTAP, puede establecer que System Availability Monitor recopile datos acerca de su dispositivo y los envíe a los Servicios de Monitoreo del Estado de Salud.

Antes de empezar

Para recopilar y realizar informes acerca de la información del estado de salud de su dispositivo, debe generar un código de activación en el GTAP, tal como se describe en la *Guía del Usuario del System Availability Monitor*.

Para activar System Availability Monitor Agent:

1 Abra SV Control Panel.

2 En la página de *Configuración*, en la sección de *System Availability Monitor*, haga clic en **Configurar**.

3 En el *Agente del monitor de disponibilidad del sistema de Genetec* ventana, haga clic **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**.

Habilitar las funciones de control de acceso y video de Security Center

El *Asistente de instalación de Security Center* El asistente lo guía a través de la configuración de las funciones principales de videovigilancia y control de acceso.

Lo que debería saber

Los ajustes que aplique en el asistente se pueden cambiar más adelante en Config Tool.

Se aplica a: Dispositivos que alojan la función de directorio, como dispositivos todo en uno

Para habilitar las características de video y control de acceso de Security Center:

1 Inicie sesión con un usuario administrador.

SUGERENCIA: Si su contraseña de Security Center es diferente de la contraseña del administrador de Windows, inicie sesión en Security Center con las credenciales de contraseña especificadas en el asistente *de configuración de Streamvault Control Panel*.

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 características más adelante en la página de *Funciones* en la vista **Configuración general** de la tarea de *Sistema*.

NOTA: Si su licencia no es compatible con alguna característica, no estará disponible en la lista.

4 En la página de *Seguridad de la cámara*, especifique el nombre de usuario y la contraseña predeterminados que se usa para todas sus cámaras y, a continuación, 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 usa 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 admite una resolución alta, utilizará la resolución más alta que pueda admitir 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 definir un horario para la grabación.

7 Haga clic en **Siguiente**.

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

9 Sobre el *Tarjetahabientes* página, seleccione cómo desea agregar sus credenciales (tarjetas) y titulares de tarjetas.

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

b) Haga 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 que realice informes puede usar la aplicación de Security Desk y ejecutar las tareas de informes más básicas, a excepción de las tareas de reconocimiento automático de placas vehiculares (ALPR, por sus siglas en inglés) de AutoVu™. Un usuario que solo tiene privilegios de informes no puede ver ningún video, controlar ningún dispositivo físico 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. Además, un supervisor puede usar tareas de mantenimiento, administrar tarjetahabientes y credenciales, modificar campos personalizados, configurar niveles de amenazas, bloquear cámaras y realizar conteos de personas.
- **Aprovisionamiento:** Un usuario de aprovisionamiento tiene casi todos los privilegios de configuración, a excepción de los siguientes: administrar funciones, macros, usuarios, grupos de usuarios, eventos personalizados, registros de actividades, niveles de amenazas 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 puede usar tareas de ALPR, configurar entidades de ALPR, crear reglas de ALPR, monitorear eventos de 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 informes ni cambiar la contraseña de Patroller.

11 Ingrese y confirme el **Contraseña**y luego haga clic en **Agregar**.

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

Cambias los perfiles de usuario en el **Usuarios** vista de *Gestión de usuarios* tarea. Para obtener más información, consulte la *Guía del Administrador de Security Center*.

12 Haga 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: El **Abra la herramienta de inscripción de unidades después de que se cierre el asistente** La opción está seleccionada por defecto. Puede borrar esta opción y abrir la Herramienta de inscripción de la unidad en otro momento haciendo clic en el acceso directo de **Inscribir cámaras y controladores** en la página de *Inicio* de SV Control Panel.

Después de que concluya

Añade unidades a tu sistema, utilizando la herramienta de inscripción de unidades.

Temas relacionados

Configurar los ajustes predeterminados de la cámara en la página 29
Crear horarios de grabación personalizados en la página 31
Página de inicio de SV Control Panel en la página 55

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™*.

Temas relacionados

Accesos directos de Config Tool en SV Control Panel en la página 55

Abrir la Herramienta de inscripción de la unidad

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

Para abrir la Herramienta de inscripción de la unidad:

- Haz una de las siguientes:
  - En la página de *Inicio* de SV Control Panel, haga clic en **Inscribir cámaras y controladores**.
  - En la página de *Inicio* de SV Control Panel, haga clic en el ícono de **Config Tool** y, a continuación, haga clic en **Tareas** > **Inscripción de la unidad**.
  - En la página de *Inicio* de SV Control Panel, haga clic en el ícono de **Config Tool** y, a continuación, haga clic en el ícono de **Agregar estado de la unidad** en la bandeja de notificaciones 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.

Para configurar los ajustes de detección:

1 Desde la página de inicio, haga clic en **Herramientas** > **Unidad de inscripción** .

2 En el *Matriculación de la unidad* cuadro de diálogo, haga clic en **Configuraciones y fabricantes** ( )

3 Configure las siguientes opciones:

- **Siempre ejecuta una búsqueda extensa** . Active esto si desea que se descubran todas las unidades del sistema.

  NOTA: También se pueden descubrir unidades de otros fabricantes porque UPnP y *Zero config* también se usan en el proceso de descubrimiento.

- **Rechazar autenticación básica** (solo unidades de video). Utilice este interruptor para habilitar o deshabilitar la autenticación básica. Esto es útil si desactivó la autenticación básica en Security Center InstallShield, pero debe volver a encenderlo para realizar una actualización de firmware o inscribir

una cámara que solo admita la autenticación básica. Para volver a activar la autenticación básica, debe cambiar el **Rechazar autenticación básica** opción a **Apagado**.

NOTA: Esta opción solo 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 28)

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.

Para agregar una unidad:

1 Desde la página de inicio, haga clic en **Herramientas** > **Unidad de inscripción** .

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 **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.

Para borrar unidades agregadas:

1 Agregue las unidades descubiertas deseadas a su sistema, vea Agregar unidades en la página 27 .

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.

Para ignorar una unidad:

1 Desde la página de inicio, haga clic en **Herramientas** > **Unidad de inscripción** .

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, consulteEliminar unidades de la lista de unidades ignoradas en la página 28 .

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 realice un descubrimiento.

Para eliminar una unidad de la lista de unidades ignoradas:

1 Desde la página de inicio, haga clic en **Herramientas** > **Unidad de inscripción** .

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 calidad de video y grabación aplicada a todas las cámaras controladas por Archiver. Al principio, estos ajustes se configuran en la página de *Configuración de la calidad de la cámara* en el asistente de instalación de Security Center.

Lo que debería saber

También puede aplicar la configuración de video y de grabación de una cámara en Config Tool usando la pestaña de **Video y grabación** de la unidad. Los ajustes realizados para una cámara en particular tienen prioridad por sobre los ajustes que se aplican en el asistente de instalación de Security Center o en la página de *Configuración predeterminada de la cámara*.

Para configurar los ajustes predeterminados de la cámara:

1 En la página de inicio de Config Tool, abra la tarea de *Video*.

2 Seleccione la función Archiver y, a continuación, haga clic en el **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 usa 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 admite una resolución alta, utilizará la resolución más alta que pueda admitir del grupo Estándar.

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

Los horarios que están disponibles incluyen los horarios que se crearon usando la vista de **Horarios** en la tarea de *Sistema* o el horario personalizado si se creó uno en el asistente de instalación de Security Center.

5 En la lista desplegable de **Modo**, seleccione un modo para el horario 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 definir un horario para 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 borrar el video después de una cantidad de días específicos. El video se borra ya sea que el almacenamiento del Archiver esté lleno o no.
- **Hora de 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.
- **Hora de grabar después de una moción:** Establezca la cantidad de segundos durante los cuales desee continuar la grabación después de un evento de movimiento. Durante este tiempo, el usuario no puede detener la grabación.
- **Duración predeterminada de la grabación manual:** 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 es usado por la acción Iniciar grabación cuando se selecciona la duración predeterminada de la grabación.

7 Haga clic en **Aplicar**.

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

Temas relacionados

Habilitar las funciones de control de acceso y video de Security Center en la página 23

Crear horarios de grabación personalizados

Crear horarios de grabación personalizados desde el asistente de instalación de Security Center para hacer que las cámaras graben en diferentes modos de grabación por un intervalo específico.

Para configurar un horario:

1 En la página de *Configuración de grabación*, haga clic en en **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.

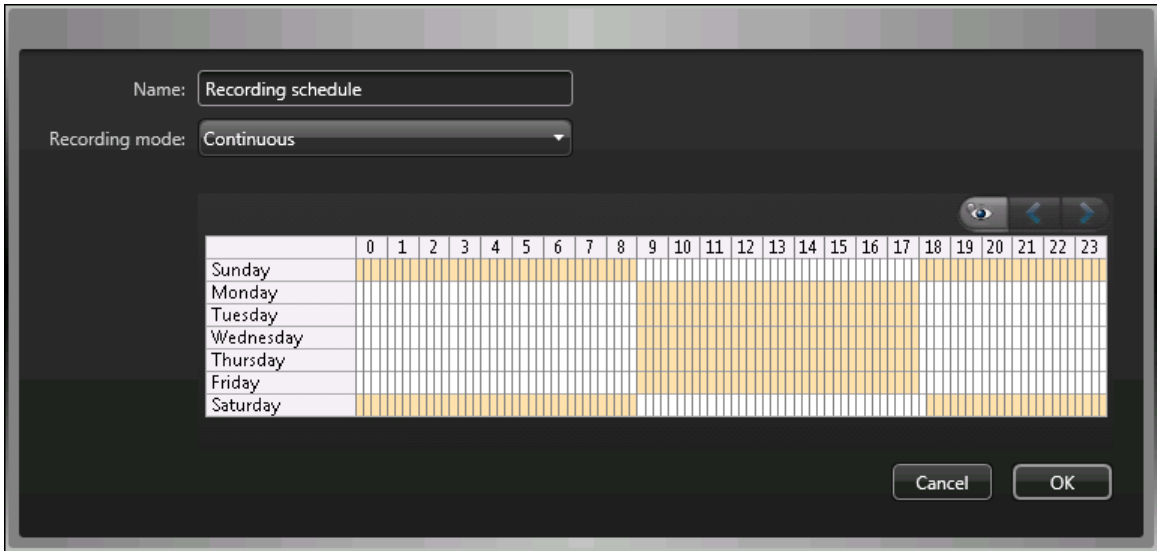
  NOTA: Cuando se usa la opción **Manual**, el movimiento no activa ninguna grabación.
- **Personalizado:** Puede definir un horario para la grabación.

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 con el botón derecho y arrastre para borrar un bloque de tiempo.
- Use las teclas del cursor para desplazarse por la cronología de 24 horas.

SUGERENCIA: Para cambiar al modo de alta resolución, en el que 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

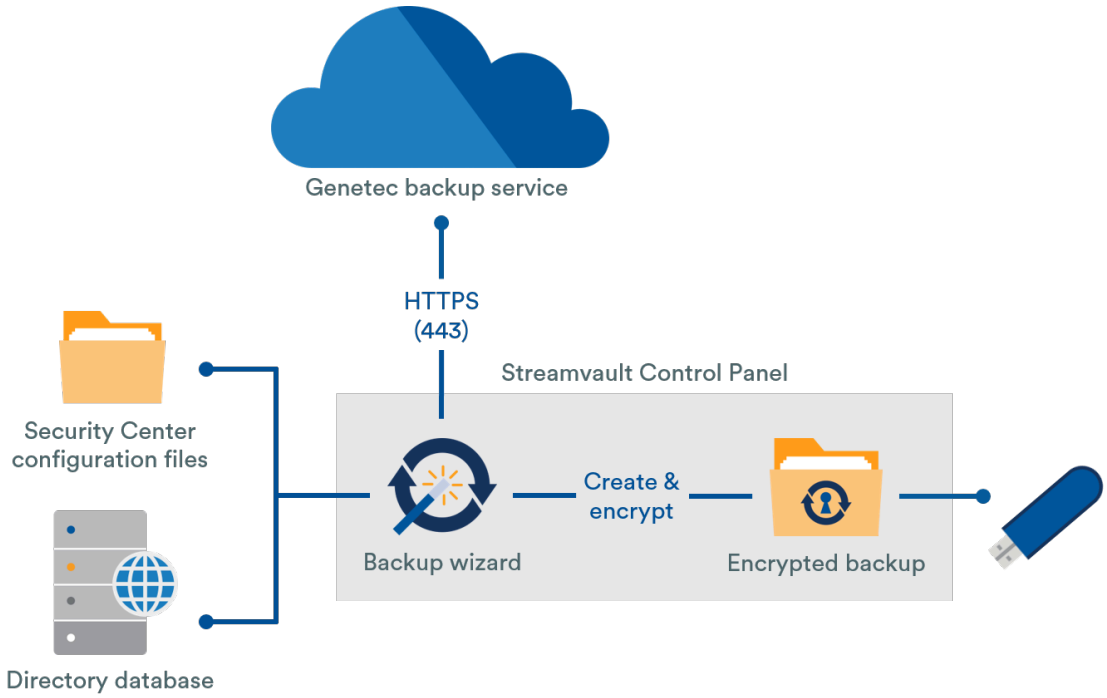
Habilitar las funciones de control de acceso y video de Security Center en la página 23

Acerca de la copia de respaldo y la restauración

Con SV Control Panel, puede realizar una copia de seguridad de los archivos de configuración y la base de datos de su Directory. Posteriormente, puede restaurarlos al mismo ID del sistema en caso de que se produzca una falla del sistema o una actualización de hardware.

Cómo crear una copia de respaldo y restaurar trabajos en SV Control Panel

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 restauración

- Cree con facilidad una copia de respaldo de sus archivos en la nube o de manera local con el asistente de *Copia de respaldo*. Si crea una copia de respaldo de archivos en la nube, se conservan las cinco últimas copias de respaldo.
- Restaure con facilidad cualquiera de las cinco copias de respaldo o cualquiera de las copias de respaldo locales de manera sencilla en la misma ID del Sistema usando el asistente de *Restauración*.
- Todos los archivos de copia de respaldo pueden encriptarse.
- El sistema se bloquea después de cinco intentos fallidos de inicio de 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 respaldo en una versión anterior de Security Center. Por ejemplo, no puede restaurar una copia de seguridad de un sistema Security Center 5.6 a un sistema Security Center 5.5.

- 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 respaldo del sistema Security Center 5.5 a un sistema Security Center 5.6.

Temas relacionados

Crear una copia de respaldo de la base de datos de su Directory en la página 33
Restaurar la base de datos de su Directory en la página 34

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

Para facilitar la configuración de su sistema después de una actualización de hardware, o para restaurar sus configuraciones después de una falla del sistema, puede hacer una copia de seguridad de su base de datos del directorio y los archivos de configuración utilizando la función de copia de seguridad y restauración.

Antes de empezar

Asegúrese de lo siguiente:

- Está instalado Security Center 5.5 o una versión posterior.
- Genetec™ Server se está ejecutando.
- Tienes una licencia válida y activa.

Lo que debería saber

- Cree con facilidad una copia de respaldo de sus archivos en la nube o de manera local con el asistente de *Copia de respaldo*. Si crea una copia de respaldo de archivos en la nube, se conservan las cinco últimas copias de respaldo.
- Solo los administradores pueden crear una copia de respaldo y todas las copias de respaldo en la nube deben autenticarse.

Para hacer una copia de seguridad de la base de datos del directorio y los archivos de configuración:

1 En SV Control Panel, haga clic en la pestaña **Configuración**.

2 En *Copia de respaldo/restauración del Directory y las configuraciones*, haga clic en **Asistente de copia de respaldo** > **Siguiente**.

3 En la página *Método de copia de respaldo*, seleccione **Nube** o **Local** y, a continuación, haga clic en **Siguiente**.

- **Nube**. Si seleccionó Nube, realice 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 pedir las credenciales para las copias de respaldo en el futuro.

  b. En la página de *Seguridad*, seleccione una de las siguientes dos opciones:

  - **Dejar que Genetec administre mi seguridad:** No necesita proporcionar una contraseña. El servicio de copia de respaldo en la nube de Genetec Inc. encripta sus datos.
  - **Usar mi propia contraseña:** Debe crear y recordar su propia contraseña para usarla más tarde para el cifrado de sus archivos de copia de seguridad.

IMPORTANTE: Si pierde u olvida su contraseña, Genetec Inc. no podrá recuperarla.

- **Local**. Si seleccionó Local, realice 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 respaldo**, aunque no se recomienda.

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 32
Restaurar la base de datos de su Directory en la página 34

Restaurar la base de datos de su Directory

Si ha creado una copia de respaldo de la base de datos de su Directory y de los archivos de configuración mediante la copia de respaldo y la restauración en SV Control Panel, puede restaurar de manera sencilla sus archivos respaldados a la misma ID del Sistema cuando ocurran eventos tales como un fallo del sistema o una actualización de hardware.

Antes de empezar

Asegúrese de lo siguiente:

- Está instalado Security Center 5.5 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 creó una copia de respaldo de sus archivos de manera local, puede restaurar cualquiera de sus copias de respaldo a la misma ID del Sistema.
- Si creó su propia contraseña para sus archivos de respaldo encriptados durante el proceso de copia de respaldo, la necesitará para restaurar sus archivos.

Para restaurar la base de datos del directorio y los archivos de configuración:

1 En SV Control Panel, haga clic en la pestaña **Configuración**.

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**.

En la página de *Autenticación*, introduzca la ID del Sistema o las credenciales del GTAP, dependiendo de cuál haya usado para autenticar la copia de respaldo. 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 33
Acerca de la copia de respaldo y la restauración en la página 32

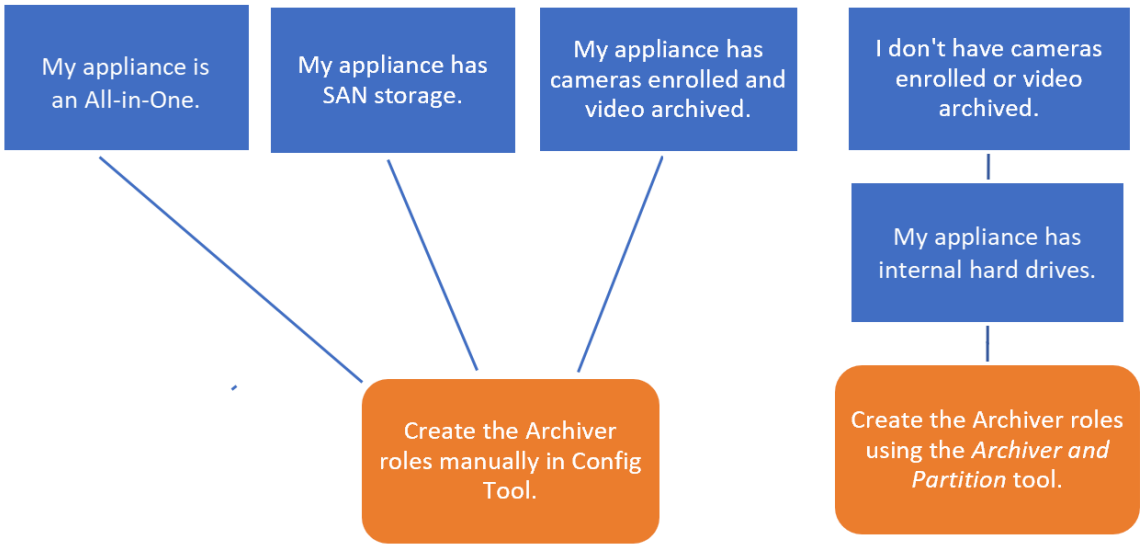
Elegir el método de creación de funciones y particiones del Archiver

Para configurar su dispositivo para la cantidad esperada de cámaras y uso de ancho de banda, debe crear suficientes roles de Archiver. Según el tipo y estado de su dispositivo, puede elegir entre dos métodos.

- Mediante la herramienta de *Funciones y Particiones de Archiver*.
- Crear particiones y funciones de Archiver de forma manual.

Elegir el método para su situación

Use el siguiente árbol de decisiones para ayudarlo a decidir qué método usar:



Acerca de la herramienta de Roles y particiones de Archiver en SV Control Panel

La herramienta de Funciones y Particiones de Archiver 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 de la serie SV-7000E, siga los pasos en Adición manual de particiones y roles de Archiver en la página 38.

Cuando la herramienta crea las particiones, todos los volúmenes locales excepto C: se borran y las funciones de Archiver existentes y las cámaras inscritas 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 1000, 2000 y 4000 de Streamvault™.

Antes de empezar

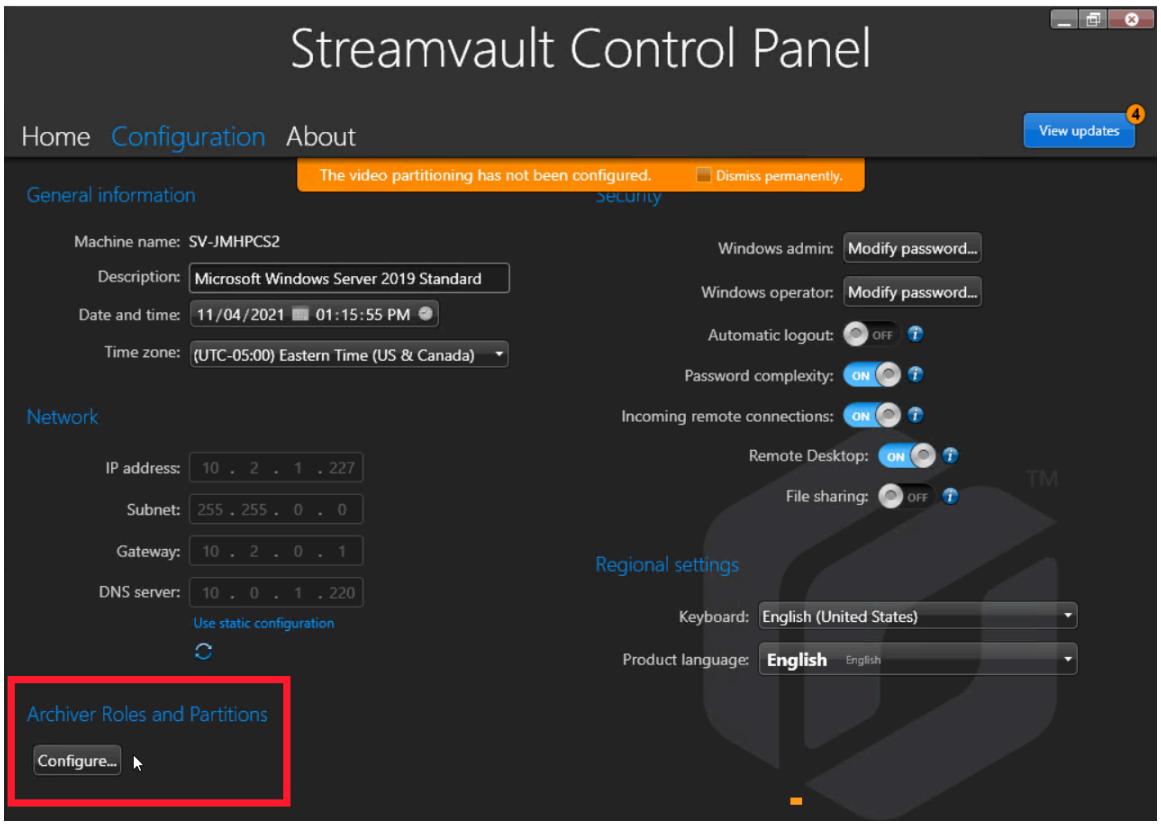
- Elija el método apropiado para crear funciones y particiones de Archiver.
- Cree una copia de respaldo de los datos importantes en la unidad que quiere particionar.

  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:.

Para crear funciones adicionales de archivador y particiones de unidades:

1 En SV Control Panel, haga clic en la pestaña **Configuración**.

2 Bajo *Funciones y particiones del archivador*, haga clic **Configurar**.



Se abre el cuadro de diálogo *Particiones y funciones de Archiver*.

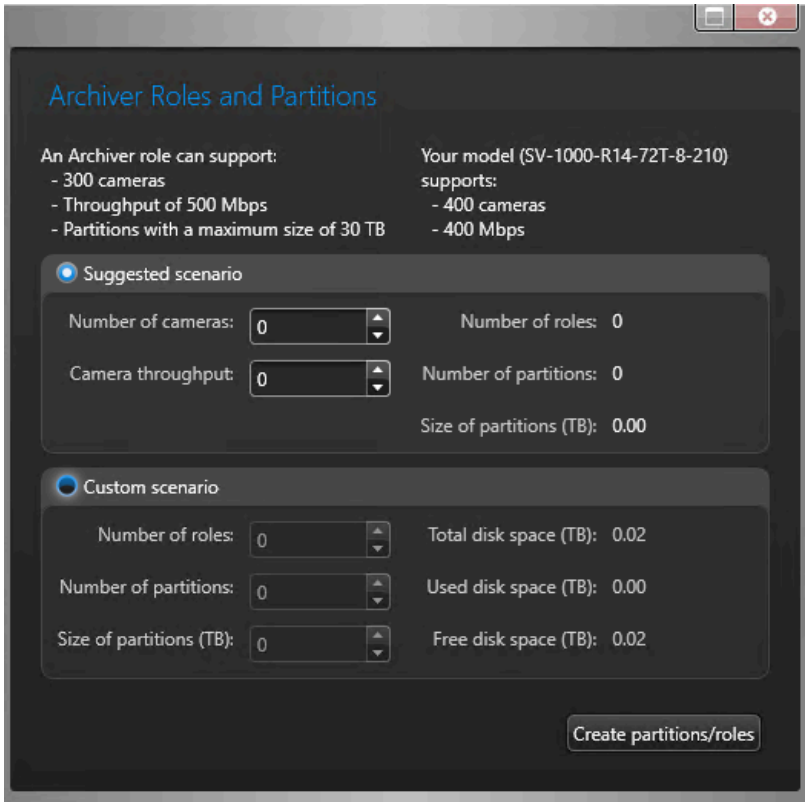
3 Seleccione una de las siguientes opciones para configurar la cantidad de funciones y particiones de Archiver:

- Para permitir que la herramienta calcule el número de funciones, el número de particiones y el tamaño de partición que necesita, seleccione la opción de **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 de Archiver que crear, seleccione la opción **Escenario personalizado**, introduzca el número de funciones de Archiver, el número de particiones y el tamaño de la partición.

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

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

4 Haga clic en **Crear particiones y funciones**.



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.

Adición manual de particiones y roles de Archiver

Para configurar su dispositivo SV-7000E o SV-300E Todo en Uno por primera vez, debe crear particiones de forma manual. También puede agregar funciones de Archiver de forma manual 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.

Para distribuir cámaras en múltiples funciones de Archiver:

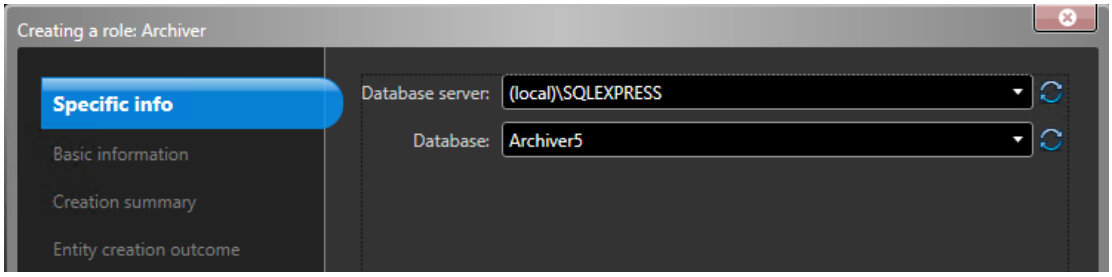
1 Si el dispositivo ya tiene cámaras registradas, video archivado o datos de control de acceso, haga lo siguiente:

a) Realice la copia de respaldo de la base de datos del Directory con SV Control Panel.

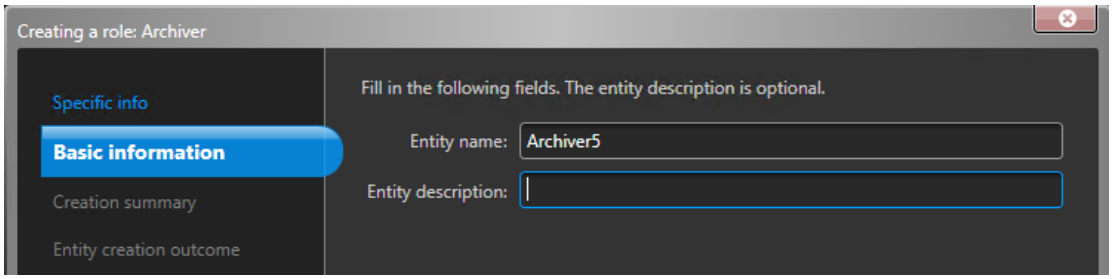
b) Generar un *Configuración de la cámara* informe para tomar una instantánea de la configuración actual de su cámara. Consulte "Visualización de la configuración de cámaras" en la *Guía del Usuario de Security Center*.

2 Cree los volúmenes que necesite para las funciones de Archiver que planee crear en el dispositivo.
   - En los dispositivos que tienen almacenamiento SAN, como los dispositivos de la serie SV-7000E, cree un número de unidad lógica (LUN, por sus siglas en inglés) para cada función de 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 *Sistema* y haga clic en la vista **Funciones**.
   b) Hacer clic **Agregar una entidad** y seleccione **archivador**.
      Se abre el asistente de creación de funciones de Archiver.
   c) En la página de *Información específica*, introduzca un nombre para la **base de datos** de funciones de Archiver y haga clic en **Siguiente**.
      Cada función de Archiver debe tener una base de datos dedicada.

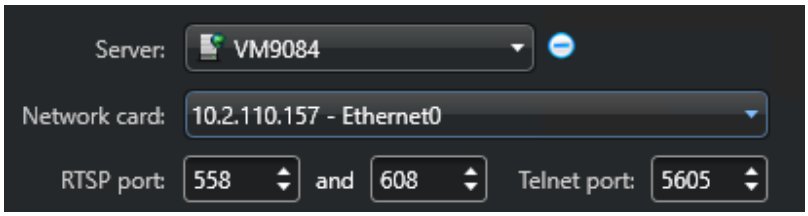


   d) En el **Información básica** sección, ingrese el **Nombre de la entidad** y haga clic **Próximo**.
      Es una buena práctica que el nombre de la base de datos de funciones de Archiver coincida con el nombre de la entidad.



   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) Hacer clic para expandir el *Servidor* y seleccione una NIC de la **Tarjeta de red** lista.
      Todas las funciones de Archiver deben utilizar la misma NIC.



   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, el Archiver B debe escribir en los discos D, E y F. Una función puede tener múltiples particiones, pero nunca debe haber dos funciones que utilicen la misma partición.
   d) Haga clic en **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) Desde la página de inicio de Config Tool, abra la tarea de *Video*.
   b) En el navegador de entidades, seleccione la función de archivador a la que desea asignar la cámara y haga clic en **Unidad de vídeo** ().
   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) Haga clic en **Aplicar**.

3

Introducción al plugin Streamvault Maintenance

Esta introducción presenta el plugin de Streamvault Maintenance y brinda información acerca de cómo configurarlo.

Esta sección incluye los temas siguientes:

Acerca de Streamvault Maintenance enchufar

El plugin Streamvault™ Maintenance se usa para monitorear la salud de sus dispositivos Streamvault y asegurar que reciba notificaciones cuando ocurran problemas.

El plugin Streamvault Maintenance incluye los siguientes componentes:

- Función Streamvault: Función de plugin que se utiliza ya sea para ejecutar el monitor de hardware o la entidad administradora. Se requiere un rol por dispositivo Streamvault que necesite monitorear.
- *Monitor de hardware de Streamvault™*: Entidad que se utiliza para definir las configuraciones de alerta de cada dispositivo Streamvault.
- *Administrador de Streamvault™*: Entidad que se utiliza para el control masivo de configuraciones de un grupo de dispositivos Streamvault. Solo se puede crear una instancia de Streamvault Manager.
- *Hardware de Streamvault™*:: Tarea de informes de Security Center que se utiliza para ver una lista de los problemas de salud que afectan a su dispositivos Streamvault.

Las configuraciones de las entidades de plugin constan de los siguientes ajustes:

- **Configuraciones de alerta**: se utiliza para definir los tipos de **Eventos**, el nivel de **Gravedad** y los tipos de **Notificaciones** que afectan a las alertas que abordan el estado de salud de sus servidores de Streamvault.
- **Destinatarios de correo electrónico**: se usa para seleccionar qué usuarios y grupos de usuarios reciben notificaciones por correo electrónico.
- **Credenciales de gestión remota**: se usa para controlar la creación de perfiles de usuario en iDRAC.
- **Integración iDRAC**: se usa para ejercer un control más preciso sobre la administración de credenciales. Esta función se puede encontrar en la pestaña de **Administración** del plugin.

  IMPORTANTE:

  - El firmware de iDRAC debe tener la versión 6.0 o una posterior.
  - El plugin de Streamvault Maintenance accede a los datos de salud mediante la comunicación fuera de banda con iDRAC. Esto significa que debe haber una conexión de red entre el puerto dedicado de iDRAC y al menos un puerto LAN si no se utiliza el uso compartido de puertos. El puerto iDRAC dedicado está deshabilitado de manera predeterminada. Para obtener más información, consulte el siguiente enlace: https://www.dell.com/support/kbdoc/en-ca/000177212/dell-poweredge-how-to-configure-the-idrac9-and-the-lifecycle-controller-network-ip.
  - La configuración mediante iDRAC no es relevante para la mayoría de los usuarios. Para obtener más información, comuníquese con el equipo de producto de Streamvault.
  - Guía aplicable para el plugin Streamvault Maintenance 1.0.

Descargar e instalar el plugin

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 lo siguiente:

- A versión compatible de Security Center está instalado.

Lo que debería saber

- **MEJOR PRÁCTICA:** Instale la función de Streamvault en todos los servidores 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:** Asegúrese de que el módulo iDRAC esté actualizado al firmware 6.00 o posterior y que el BIOS del servidor esté actualizado a la versión más reciente antes de continuar.
- El plugin solo es compatible con servidores que ejecuten el software del servidor de Security Center.
- **NOTA:** El plugin de Streamvault Maintenance viene preinstalado en todos los servidores de 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 plugin estuviera disponible, o si se desinstaló, siga estos pasos para instalarlo.

Para instalar el plugin:

1. Abra la página de Descarga de Productos del GTAP.
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. Sigue las instrucciones de instalación.
7. En la página de *Asistente de Instalación Completado*, haga clic en **Finalizar**.
   IMPORTANTE: La opción de **Reiniciar Genetec™ Server** está seleccionada de manera 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 todas las instancias 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.

Configuración de privilegios de usuario para Streamvault

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

En la tarea de *Administración de usuarios* de la Config Tool, puede configurar o modificar los privilegios de usuario o grupo de usuarios en la página de *Privilegios* 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* .

NOTA: Para obtener una lista de todos los privilegios disponibles de Security Center, consulte la hoja de cálculo de Privilegios de Security Center. 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	• 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	• 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 del plugin

Antes de configurar y utilizar el plugin, debe crear la función del plugin Streamvault™ Maintenance en Config Tool.

Antes de empezar

Descargue e instale el plugin.

Lo que debería saber

El plugin de Streamvault Maintenance contiene dos funciones de plugin:

- 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 necesita un monitor de Hardware de Streamvault™ por dispositivo de Streamvault™.
- Streamvault manager: La entidad Streamvault™ manager se usa para controlar las configuraciones de alertas para un grupo de entidades de monitor de hardware de Streamvault™. Solo se admite un Streamvault™ manager por sistema.
- **NOTA:** Si los servidores de Directory son máquinas virtuales o servidores que no son de Streamvault, debe crear una función para estos servidores solo si desea utilizar la entidad Manager.

Para crear una función de plugin:

1 Desde la página de inicio de Config Tool, abra la tarea de *Plugins*.

2 En la tarea de *Plugins*, haga clic en **Agregar una entidad** () y seleccione **Plugin**.

Se abre el asistente de creación de plugins.

3 En la página *Información específica*, seleccione el servidor en el que está alojada la función del plugin y el tipo de plugin, y luego haga clic en **Siguiente**.

Si no utiliza servidores de expansión en su sistema, no se muestra la opción **Servidor**.

4 En la página de *Información básica*, especifique la información de la función:

a) Introduzca el **Nombre de la entidad**.

b) Introduzca la **Descripción de la entidad**.

c) Seleccione la **Partición** para la función de plugin.

Si no utiliza particiones en su sistema, no se muestra la opción **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.

Configurar la entidad de monitor 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.

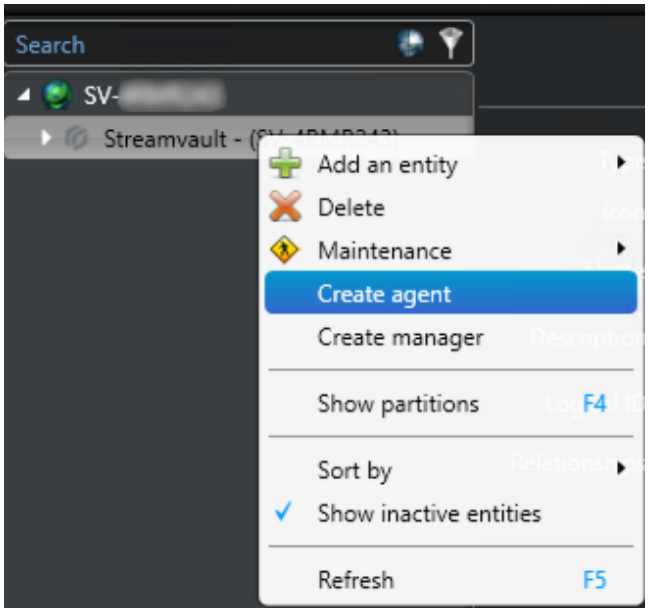
Antes de empezar

- Inscriba sus dispositivos Streamvault.
- Crear la función del plugin de Streamvault.
- **IMPORTANTE:** Se crea un agente de forma automática en cada servidor de Streamvault que aloje una función de Streamvault. Si el agente no está presente en su sistema después de la creación de la función, debe crear el agente de forma manual.

Para configurar una entidad de monitor de hardware de Streamvault:

1 En Config Tool, navegue hasta la tarea de *Plugins* y seleccione la función del plugin de Streamvault.

2 Haga clic derecho en la función del plugin de Streamvault y haga clic en **Crear monitor de hardware**.

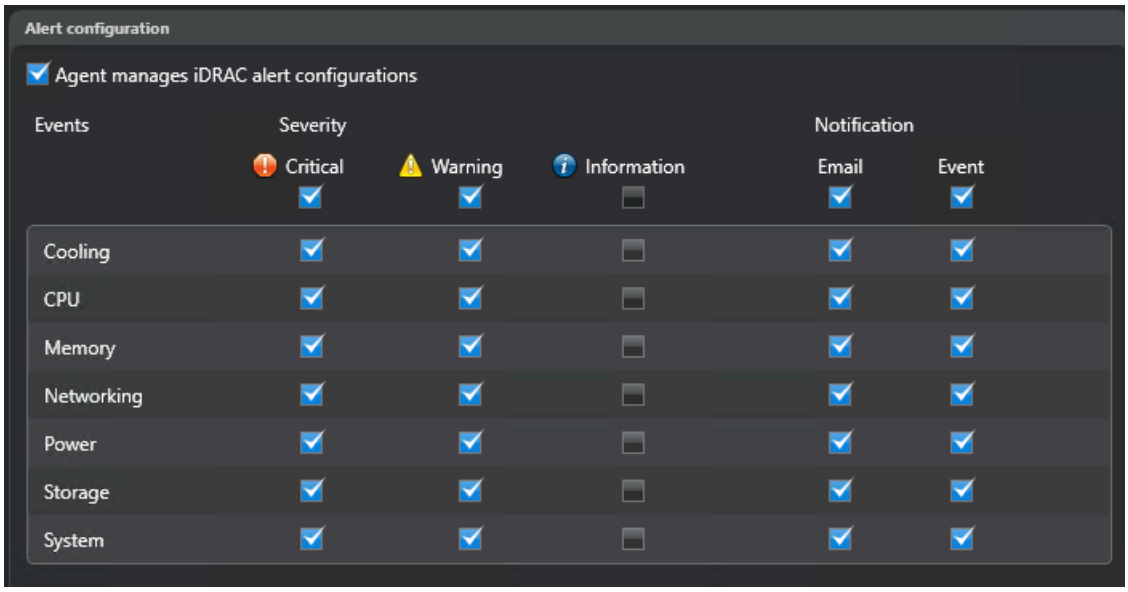


3 Desde la pestaña de **Identidad**, introduzca un nombre para el Monitor de hardware de Streamvault en el campo de **Nombre**.

4 Desde el **General** pestaña, configure lo siguiente:

a) Para administrar las configuraciones de alerta a través de las configuraciones de la función del Monitor de hardware de Streamvault, active la casilla de verificación **El agente administra las configuraciones de alertas de iDRAC**.

b) En el sección de **Notificaciones de alerta**, active las casillas de verificación que correspondan a los tipos de **Eventos**, el nivel de **Gravedad** y los tipos de **Notificaciones** que desee incluir para este Monitor de hardware de Streamvault.



5 En el **Destinatarios de correo electrónico** sección, elija qué usuarios y grupos de usuarios reciben notificaciones por correo electrónico cuando una condición en el **Configuración de alertas** se cumple el apartado.

6 (Opcional) En la sección de **Credenciales de gestión remota**, active la casilla de verificación de **El Agente gestiona la cuenta de iDRAC** para gestionar las credenciales de manera directa a través del plugin.

7 (Opcional) En la sección de **Credenciales de gestión remota**, desactive la casilla de verificación de **El Agente gestiona la cuenta de iDRAC** para usar iDRAC para controlar la creación de usuarios y contraseñas.

8 (Opcional) Si desactivó la casilla de verificación de **El Agente gestiona la cuenta de iDRAC**, vaya a la pestaña de **Gestión** y configure las credenciales de manera directa en iDRAC.

9 (Opcional) En la sección de **puerto de entrada**, puede cambiar el puerto predeterminado de 65115 a su opción preferida. Para más información, ver Puertos predeterminados utilizados por Streamvault en la página 4.

Configurar de una entidad de Streamvault manager

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 y establecer notificaciones para que se generen cuando ocurran problemas. La entidad Streamvault manager solo se usa para esto y es opcional.

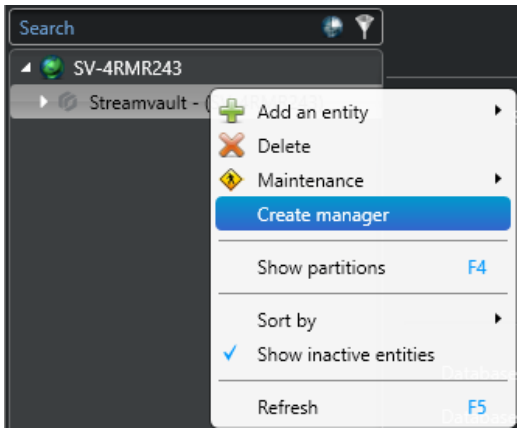
Antes de empezar

- Inscriba sus dispositivos Streamvault.
- Crear la función del plugin de Streamvault.

Para configurar de una entidad de Streamvault manager

1 En Config Tool, navegue hasta la tarea de *Plugins* y seleccione la función del plugin de Streamvault.

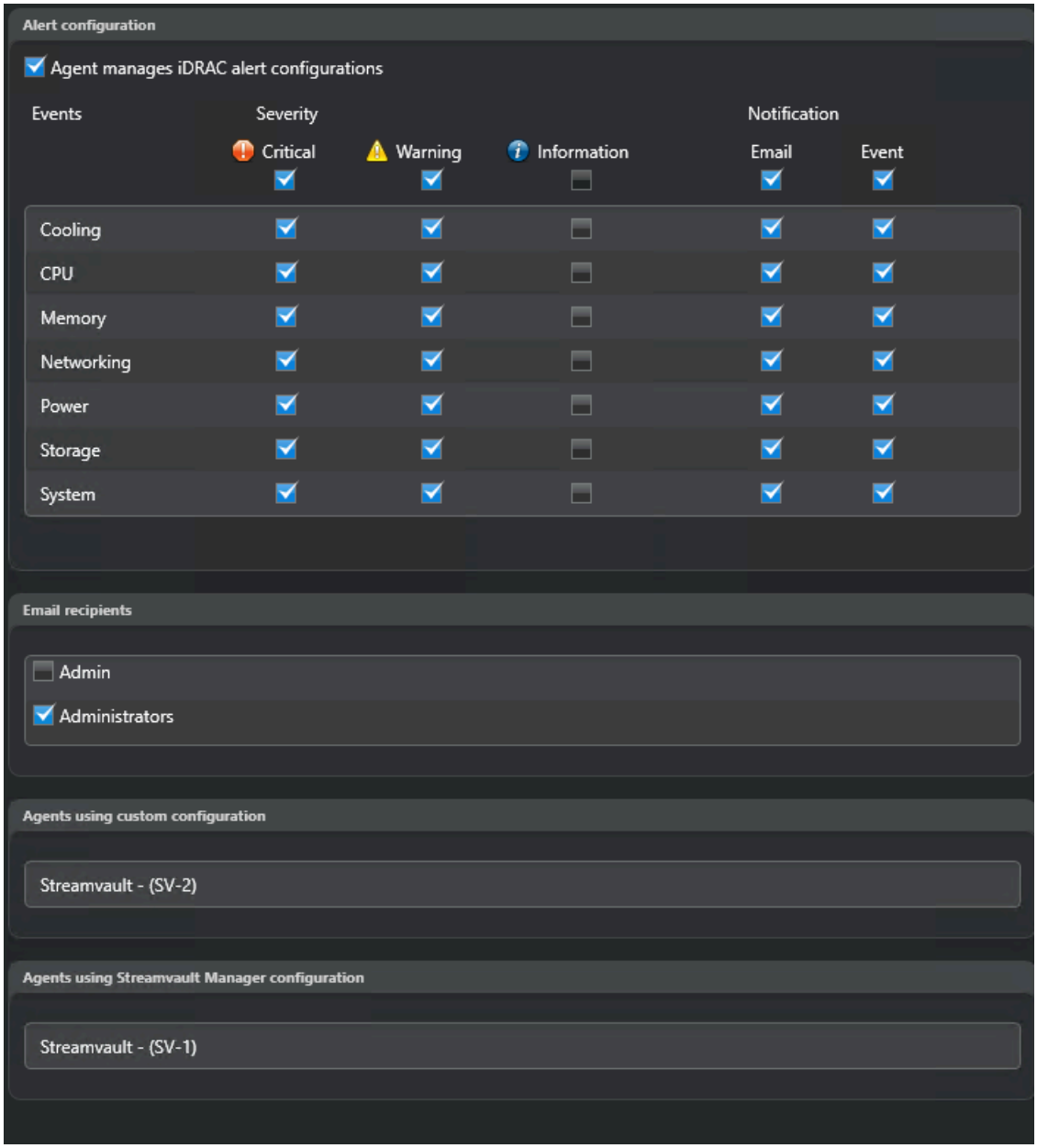
2 Haga clic con el botón derecho en la función del plugin de Streamvault y haga clic en **Crear administrador**.



3 Desde el **General** pestaña, configure lo siguiente:

a) Para gestionar las configuraciones de alertas a través de las configuraciones de Streamvault manager, active la casilla de verificación de **El agente gestiona las configuraciones de alerta de iDRAC**.

b) En el sección de **Notificaciones de alerta**, active las casillas de verificación que correspondan a los tipos de **Eventos**, el nivel de **Gravedad** y los tipos de **Notificaciones** que desee incluir para las instancias del plugin Streamvault Maintenance controladas por este Streamvault manager.



NOTA: Las instancias de Streamvault cuyas configuraciones fueron establecidas por Streamvault manager se muestran en la sección de **Agentes que utilizan la configuración de Streamvault manager**.

4 En el **Destinatarios de correo electrónico** sección, elija qué usuarios y grupos de usuarios reciben notificaciones por correo electrónico cuando una condición en el **Configuración de alertas** se cumple el apartado.

5 (Opcional) En la sección de **Credenciales de gestión remota**, active la casilla de verificación de **El Agente gestiona la cuenta de iDRAC** para gestionar las credenciales de manera directa a través del plugin.

6 (Opcional) En la sección de **Credenciales de gestión remota**, desactive la casilla de verificación de **El Agente gestiona la cuenta de iDRAC** para usar iDRAC para controlar la creación de usuarios y contraseñas.

7 (Opcional) Si desactivó la casilla de verificación de **El Agente gestiona la cuenta de iDRAC**, vaya a la pestaña de **Gestión** y configure las credenciales de manera directa en iDRAC.

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.

Para ver el estado de salud de sus dispositivos Streamvault:

1 Desde la página de inicio, abra el *Hardware de bóveda de flujo* tarea.

2 En el filtro de consulta de **Intervalo**, defina el período 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 lo que está causando el problema.

NOTA: Para obtener más información acerca de la creación de informes, consulte el Resumen general del espacio de trabajo de la tarea de informes.

4

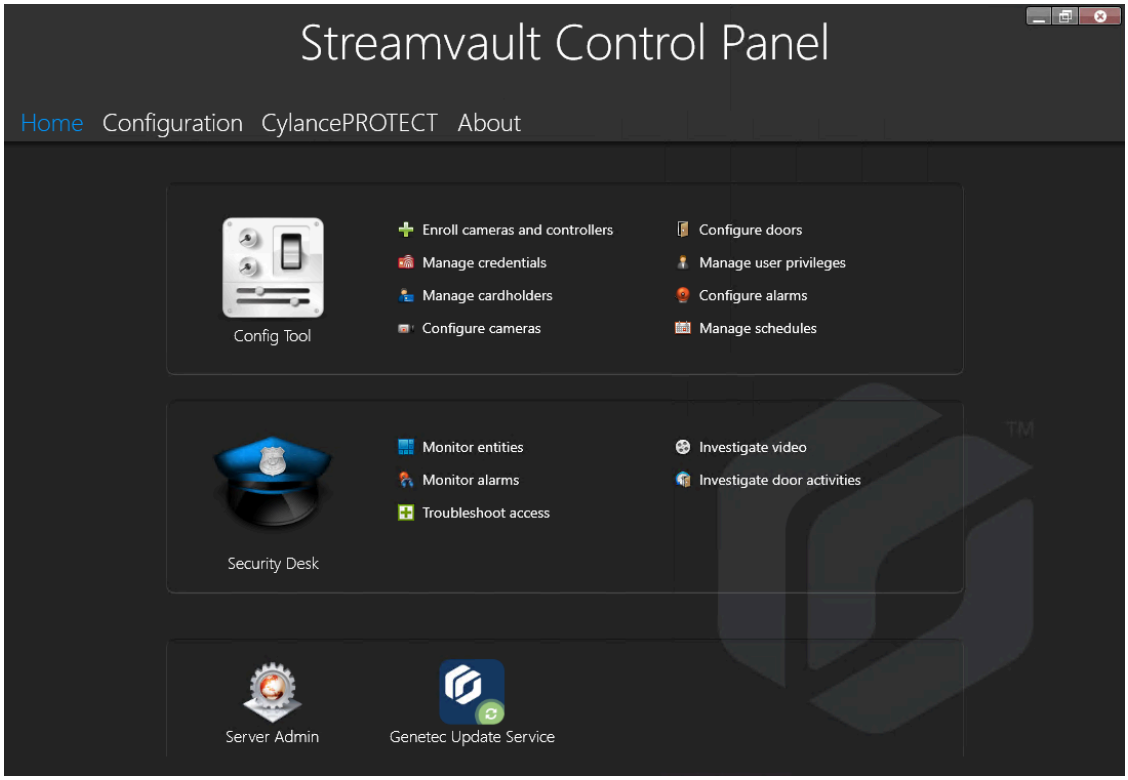
Referencia de SV Control Panel

Estas páginas de referencia lo ayudan a entender SV Control Panel.

Esta sección incluye los temas siguientes:

Página de inicio de SV Control Panel

Utilizar el *Hogar* para acceder a las tareas básicas requeridas 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.



De manera alternativa, puede hacer clic en los accesos directos de Config Tool o de Security Desk para abrir las tareas asociadas.

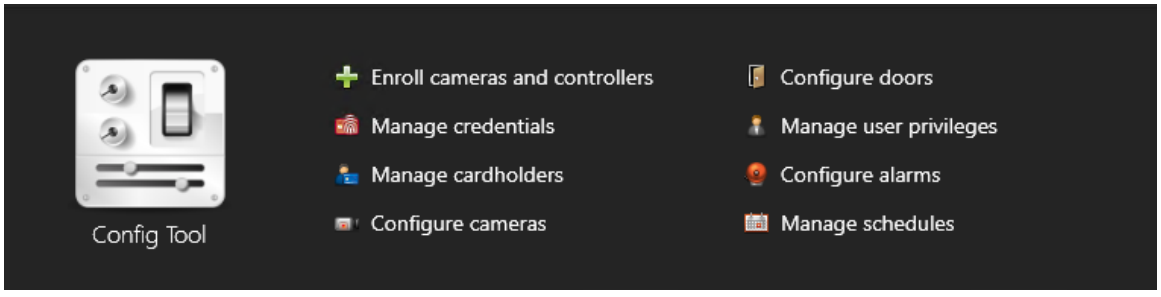
Para los sistemas que se ejecutan en modo Cliente, el acceso directo de Server Admin no está disponible. De la misma manera, los accesos directos de Config Tool y Security Desk también están limitados.

NOTA: Si su sistema no está activado, se le notifica mediante un banner rojo. Haga clic en **El sistema no está activado. Haga clic aquí para activar.** para abrir el asistente *de activación de Streamvault Control Panel*.

Accesos directos de Config Tool en SV Control Panel

Use los accesos directos para abrir las tareas principales en la aplicación de Config Tool.

Los accesos directos que están disponibles dependen de las opciones de licencia que tenga.



- **Herramienta de configuración:** Haga clic en el ícono para abrir Config Tool.

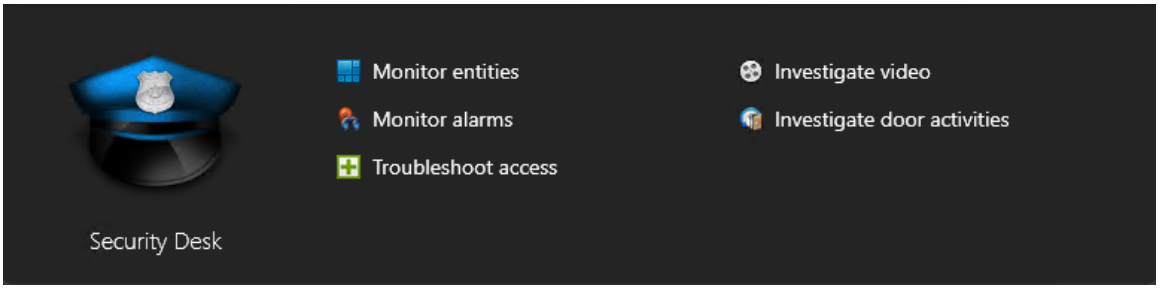
Temas relacionados

Acerca de la Herramienta de Inscripción de la Unidad en la página 26

Accesos directos de Security Desk en SV Control Panel

Use los accesos directos para abrir las tareas principales en la aplicación de Security Desk.

Los accesos directos que están disponibles dependen de las opciones de licencia que tenga.



- **Escritorio de seguridad:** Haga clic en el ícono para abrir Security Desk.
- **Supervisar entidades:** Haga clic para abrir la tarea de *Monitorear* para monitorear los eventos del sistema en tiempo real.
- **Monitorear alarmas:** Haga clic para abrir la tarea de *Monitorear alarmas* para monitorear y responder a las alarmas activas, y ver las alarmas pasadas.
- **Acceso a la resolución de problemas:** Haga clic para abrir la herramienta del Solucionador de problemas de acceso para 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:** Haga clic en abrir la tarea de *Archivos* para buscar archivos de videos.

  NOTA: Este acceso directo no está disponible para los sistemas que se ejecutan en modo Cliente.
- **Investigar actividades de puertas:** Haga clic para abrir la tarea de las *Actividades de las puertas* para investigar los eventos ocurridos en puertas seleccionadas.

  NOTA: Este acceso directo no está disponible para los sistemas que se ejecutan en modo Cliente.

Server Admin en SV Control Panel

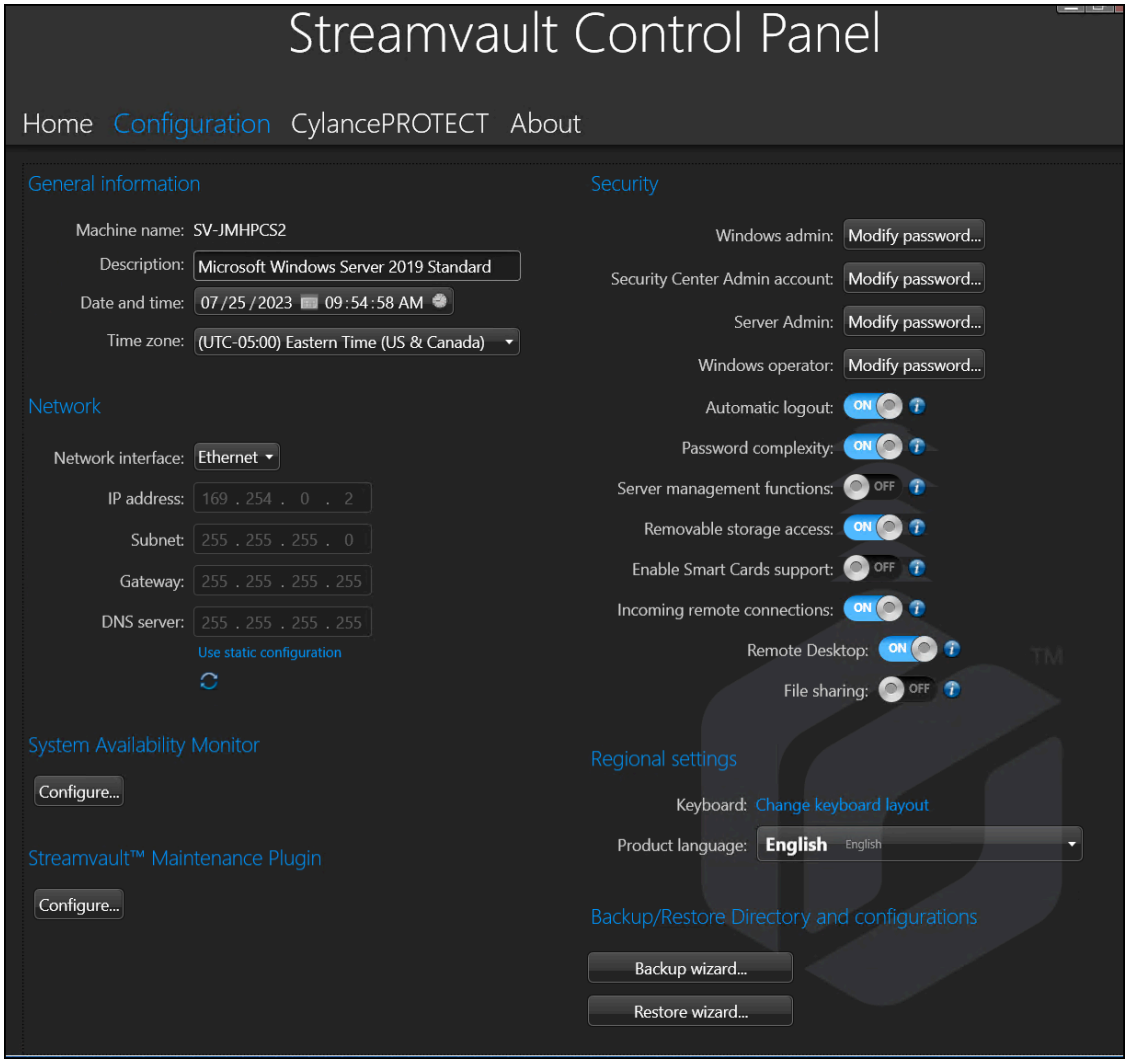
Use la aplicación de Server Admin para aplicar una licencia de manera manual o para ver y cambiar la configuración del servidor.

Genetec Update Service en SV Control Panel

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

Página de Configuración de SV Control Panel

Utilice la página de *Configuración* de SV Control Panel para modificar la configuración general, como la *configuración de la red*, la *configuración de System Availability Monitor*, las *cuentas de usuario*, y los *ajustes regionales*.



Para sistemas que se ejecutan en un servidor de expansión o en modo Cliente, el *Monitor de disponibilidad del sistema*, *Características*, y *Copia de seguridad/Restaurar directorio y configuraciones* las secciones no están disponibles. Del mismo modo, en la sección de *Seguridad*, solo se pueden modificar las contraseñas para las opciones de **Administrador de Windows** y **Operador de Windows**.

Configuración de la información general

Use la sección de *Información general* de la página de *Configuración* para cambiar los ajustes, tales 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 una zona horaria de la lista desplegable.

Configuración de red

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

- **Interfaz de red:** Seleccione la tarjeta de red que desea configurar.

  NOTA: Esta opción no está disponible cuando solamente hay una tarjeta de red conectada.
- **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.
- **Usar configuración estática:** Haga clic cuando no desee que el servidor DHCP asigne la dirección IP de forma dinámica. De manera predeterminada, el Protocolo de Configuración Dinámica de Anfitrión (DHCP) se usa para asignar de manera automática la dirección IP, la subred, la puerta de enlace y el servidor DNS.
- **Actualizar (solo para el DHCP):** Haga clic para actualizar su configuración de DHCP y obtener una nueva dirección IP.

Configuración de System Availability Monitor

Use la sección de *System Availability Monitor* de la página de *Configuración* 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 los sistemas que se ejecutan en un servidor de expansión o en modo Cliente.

Información de características

Utilizar el *Características* sección de la *Configuración* para mostrar y activar las funciones adicionales que compró.

Se pueden habilitar las siguientes características:

- Security Center Mobile
- Alambre blando Synergis™

NOTA: Si Security Center Mobile o Synergis Softwire no están instalados, las respectivas opciones no se verán en la sección de *Características*. Security Center Mobile solo está disponible para Security Center 5.7 y versiones anteriores. Para los sistemas que ejecutan Security Center 5.8 de disponibilidad general (GA, por sus siglas en inglés) y versiones posteriores, Security Center Mobile se activa en Config Tool.

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

Seguridad

Use la sección de *Seguridad* en la página de *Configuración* para cambiar algunos de los ajustes de la cuenta de usuario y del sistema de seguridad de 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 aplicaciones de Security Center.

Defina una contraseña para cada producto:

- **Administrador de Windows:** La contraseña del usuario administrador para Windows.
- **aplicaciones cliente:** 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.
- **Cierre de sesión automático:** Active esta opción para configurar Windows para que cierre la sesión de un usuario después de 15 minutos de inactividad.
- **Complejidad de la contraseña:** Active esta opción para solicitar una contraseña compleja de al menos 10 caracteres para los usuarios de Windows.
- **Funciones de gestión del servidor:** Active esta opción para permitir funciones como agregar funciones y otras tareas con aplicaciones como *Windows Admin Center*, *Server Manager* o *Windows PowerShell*.
- **Acceso de almacenamiento que se puede eliminar:** Active esta opción para habilitar el acceso a una memoria USB o un disco duro USB conectado desde Windows.

  NOTA: Los usuarios con privilegios administrativos tienen acceso al almacenamiento extraíble de forma automática.
- **Habilitar compatibilidad con las tarjetas inteligentes:** Active esta opción para crear o utilizar un lector de tarjetas inteligentes con la aplicación Security Desk. Para evitar que el software malintencionado afecte al dispositivo, esta opción se ha desactivado de forma predeterminada.
- **Conexiones remotas entrantes:** Active esta opción para permitir el acceso a las conexiones de *Escritorio Remoto* y la función de compartir archivos al dispositivo desde su red de computadoras. Para evitar que el software malintencionado afecte al dispositivo, esta opción se ha desactivado de forma predeterminada.
- **Escritorio Remoto:** Active esta opción para permitir que las personas de su red inicien sesión en el dispositivo mediante una aplicación de *Escritorio Remoto*. La opción de **Conexiones remotas entrantes** también debe estar habilitada para permitir el acceso al *Escritorio Remoto*. Para evitar que el software malintencionado afecte al dispositivo, esta opción se ha desactivado de forma predeterminada.
- **Uso compartido de archivos:** Active esta opción para compartir archivos y carpetas que se encuentran en el dispositivo con personas en su red. La opción de **Conexiones remotas entrantes** también debe estar habilitada para permitir el uso compartido de archivos. Para evitar que el software malintencionado afecte al dispositivo, esta opción se ha desactivado de forma predeterminada.

Configuración regional

Use la sección de *Configuración regional* en la página de *Configuración* para cambiar la configuración de idioma de la distribución de teclado de su sistema.

- **Cambiar la distribución del teclado:** Haga clic para abrir el *Panel de Configuración de Windows* para cambiar la distribución de su teclado.

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

NOTA: SV Control Panel solo está disponible en inglés.

Copia de respaldo y restauración

Utilizar el *Copia de seguridad/Restaurar directorio y configuraciones* sección sobre el *Configuración* página para acceder a la *Respaldo* mago y *Restaurar* mago.

La copia de respaldo y restauración es una característica de SV Control Panel que puede usar para crear una copia de respaldo de manera segura de la base de datos de su Directory y los archivos de configuración y, luego, restaurarlos a la misma ID del Sistema ante un evento de fallo del sistema o una actualización de hardware. Esta función no realiza una copia de seguridad de su archivo de licencia, archivos de video u otras bases de datos.

Esta sección no está disponible para los 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 más información, ver Puertos predeterminados utilizados por Streamvault en la página 4.

Temas relacionados

Acerca de la copia de respaldo y la restauración en la página 32

Crear una copia de respaldo de la base de datos de su Directory en la página 33

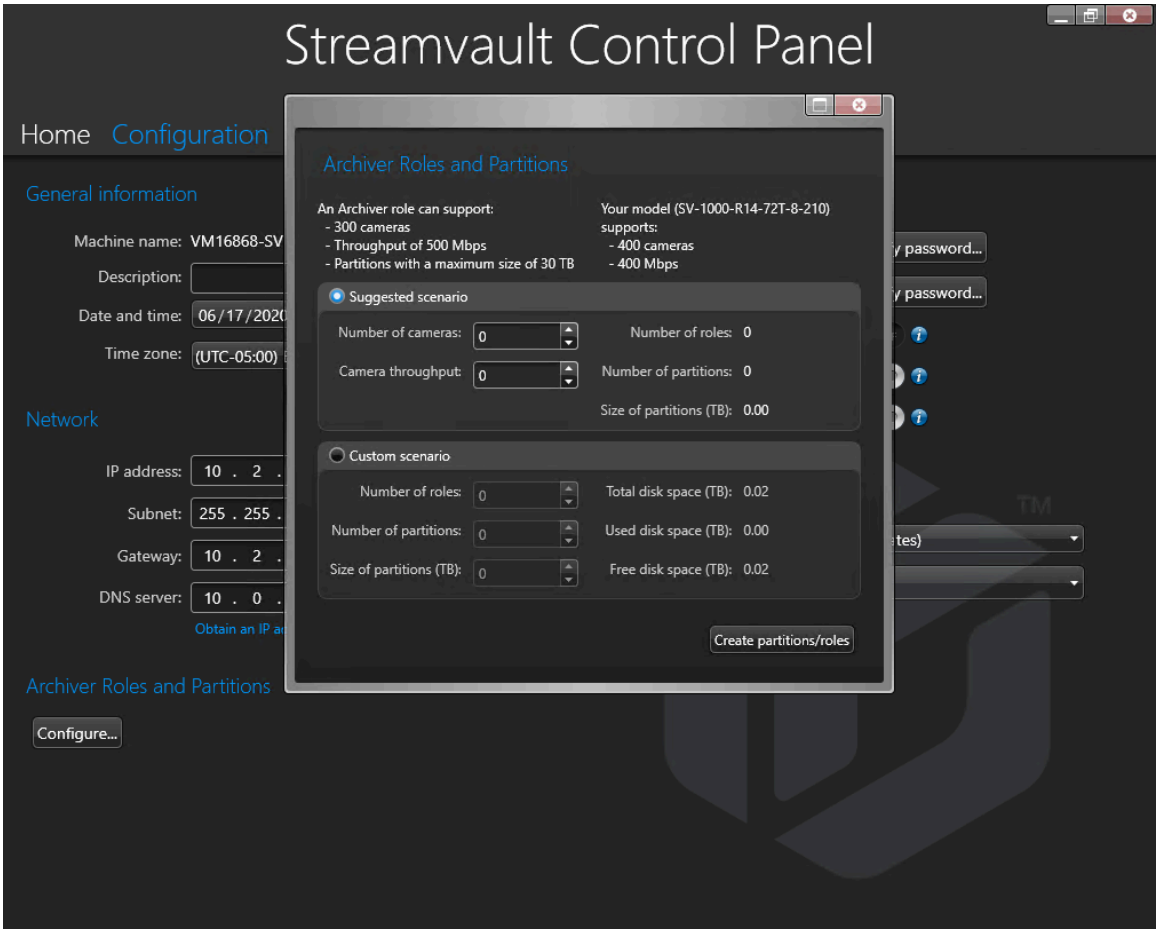
Restaurar la base de datos de su Directory en la página 34

Particiones y Funciones del Archiver

Utilizar el *Funciones y particiones del archivador* sección sobre el *Configuración* página para ampliar el número máximo de cámaras admitidas en su sistema.

La característica de Particiones y Funciones del Archiver es una característica de SV Control Panel que puede usar para configurar sistemas que requieren más que la cantidad máxima de cámaras y productividad que admite una sola función del Archiver.

Esta sección solo está disponible para los sistemas que se ejecutan en un servidor de expansión con Security Center 5.8 y versiones posteriores.



- **Un rol de archivador 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, las particiones y el tamaño de partición necesarios para la cantidad deseada de cámaras y productividad.
- **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 36.

Página de CylancePROTECT de SV Control Panel

Use la página de CylancePROTECT para ver información acerca de Cylance y elija el modo en el cual el dispositivo de Streamvault™ se comunica con la Consola de Cylance en la nube.

Puedes elegir entre las siguientes opciones:

- **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.

IMPORTANTE: Cuando CylancePROTECT está desactivado, no se puede cambiar entre **Desconectado** y **En línea**. Para cambiar esta configuración, debe restablecer la imagen del software en su dispositivo.

PRECAUCIÓN: Si cambia de opción, será necesario reiniciar la computadora, lo que causará tiempo de inactividad del sistema.

Para tener acceso a los registros y las características avanzadas de su sistema, seleccione la opción de **Ejecutar CylancePROTECT en Modo de IU Avanzado**.

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 de la licencia, información del Acuerdo de Mantenimiento de Software (SMA, por sus siglas en inglés), enlaces al Portal de Asistencia Técnica de Genetec™ (GTAP, por sus siglas en inglés) y enlaces a la documentación del producto.

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

Información de licencia

Utilizar el *Licencia* sección de la *Acerca de* página para mostrar información sobre 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.
- **Numero de lectores:** Muestra cuántos lectores admite su sistema.
- **Número de tarjetahabientes:** Muestra cuántos tarjetahabientes admite su sistema.
- **Vídeo:** Muestra si las características de video son compatibles o no.
- **Número de cámaras:** Muestra cuántas cámaras admite su sistema.
- **Mostrar licencia completa:** Haga clic para mostrar información adicional de la licencia.

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

Temas relacionados

Activar su licencia de Security Center en un dispositivo en la página 18

Información sobre el Acuerdo de Mantenimiento de Software

Utilizar el *SMA* sección de la *Acerca de* página para mostrar información sobre el Acuerdo de mantenimiento de software.

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

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

Información del sistema

Utilizar el *Sistema* sección de la *Acerca de* página para mostrar información sobre el sistema.

- **Fabricante:** Muestra el fabricante del hardware.
- **Modelo de hardware:** Muestra el modelo de hardware.
- **Revisión de software:** Muestra la versión o una imagen del software.
- **ID del sistema:** Muestra el número de ID 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

Use la sección de *Ayuda* de la página de *Acerca de* para tener acceso a enlaces útiles al Portal de Asistencia Técnica de Genetec™ (GTAP, por sus siglas en inglés) 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 el 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 de SV Control Panel*, que también contiene las notas de la versión de SV Control Panel.
- **Escritorio de seguridad:** Haga clic en el enlace para abrir la *Guía del usuario de Security Center*.

5

Recursos adicionales

Esta sección incluye los temas siguientes:

Crear una memoria USB de restablecimiento de fábrica.

Para restablecer la imagen de un dispositivo Streamvault™ SV-100E, SV-300E, SV-350E, o de un servidor Streamvault o dispositivo de estación de trabajo, debe preparar una memoria USB de arranque que contenga la imagen del software Streamvault requerida.

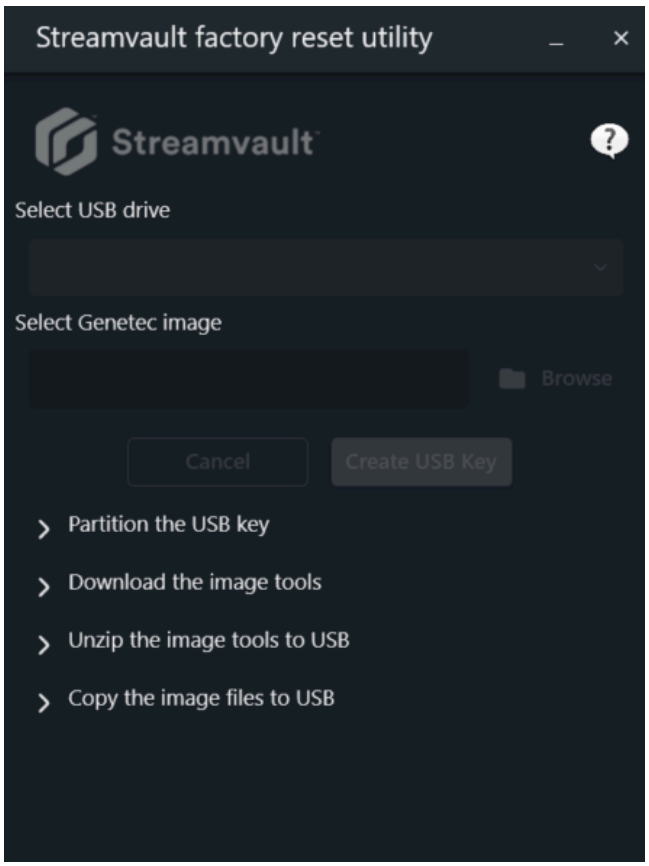
Antes de empezar

- Descargue la *Utilidad de restablecimiento de fábrica de Streamvault* desde la sección de Descargas de la *Guía del Usuario del Dispositivo Streamvault* en TechDoc Hub.
- Antes de abrir la herramienta de *Utilidad de restablecimiento de fábrica de Streamvault*, descomprima las imágenes de copia de seguridad en una carpeta de Windows.
- Asegúrese de tener una memoria USB con un mínimo de 32 GB de almacenamiento.

Vea este video para aprender cómo crear una memoria USB para restablecimiento de fábrica.

Para crear una memoria USB de arranque con la imagen de software requerida en la *Utilidad de restablecimiento de fábrica de Streamvault*:

1 Desde la lista **Seleccionar memoria USB**, seleccione una memoria USB que tenga al menos 32 GB de almacenamiento.



2 En la sección *Seleccione la imagen de Genetec*, haga clic en **Examinar** y seleccione el archivo *.swm* requerido.

- Para dispositivos All-in-One, seleccione cualquiera de los archivos descomprimidos de la carpeta *wim*.
- Para estaciones de trabajo y servidores, seleccione la imagen requerida de la carpeta *<service tag number>*.

3 Haga clic en **Crear memoria USB**.

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

Cuando se complete la descarga, verá un mensaje en la herramienta de la *Utilidad de restablecimiento de fábrica de Streamvault* que le informe que la memoria USB se creó con éxito.

Después de que concluya

- Para un dispositivo SV-100E, SV-300E o SV-350E, restablezca el software en el dispositivo.
- Para una estación de trabajo o dispositivo de servidor, restablezca la imagen del dispositivo Streamvault con la memoria USB de arranque.

Garantía de producto de su dispositivo Streamvault

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

Para ver una descripción detallada de los términos y condiciones de la garantía de producto de Genetec™, consulte el Resumen General de la Garantía de los Productos de Genetec™.

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.

Consulte las *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 edición de Windows e información de certificado estampada para productos que contienen versiones integradas de software de Microsoft.

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, podría ser necesario reducir el nivel de protección del dispositivo.

Para obtener un resumen general de la disponibilidad de productos, el soporte y los servicios disponibles, consulte la página de Ciclo de Vida de Productos en el GTAP.

Encontrar la ID de sistema y el número de revisión de software de un dispositivo Streamvault

Al comunicarse con el Soporte Técnico de Genetec™, necesita el ID del sistema y el número de revisión de software (versión de imagen) del software de Genetec instalado en el dispositivo.

Antes de empezar

Inicie sesión en Windows como administrador.

Lo que debería saber

Además de la ID de sistema y el número de revisión de software, el Soporte Técnico de Genetec podría solicitarle el número de certificación y el número de serie. Para encontrar esta información, busque una etiqueta en el dispositivo Streamvault.

Para encontrar el ID del Sistema y la versión de imagen de su dispositivo:

1 Desde el escritorio de Windows, abra **Genetec™ SV Control Panel**.

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 el número de **Revisión de software**.

Temas relacionados

Restablecimiento de fábrica en un dispositivo SV-100E, SV-300E o SV-350E en la página 74

Realizar un restablecimiento de fábrica en un dispositivo Streamvault de estación de trabajo o servidor en la página 78

Permitir compartir archivos en un dispositivo Streamvault

Para compartir los archivos y 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.

Para habilitar el uso compartido de archivos en su dispositivo:

1 Sobre la página de *Configuración* de SV Control Panel:
   - Enciende el **Conexiones remotas entrantes** opción.
   - Active la opción de **Uso compartido de archivos**.

2 Haga clic en **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.

Para permitir conexiones a Escritorio Remoto con su dispositivo Streamvault™:

1 Sobre la página de *Configuración* de SV Control Panel:
   - Enciende el **Conexiones remotas entrantes** opción.
   - Active la opción de **Escritorio Remoto**.

2 Haga clic en **Aplicar**.

Temas relacionados

El Escritorio Remoto no se puede conectar a un dispositivo Streamvault en la página 83

6

Solución de problemas

Esta sección incluye los temas siguientes:

Restablecimiento de fábrica en un dispositivo SV-100E, SV-300E o SV-350E

Si el software de un dispositivo SV-100E, SV-300E o SV-350E no inicia o deja de funcionar según lo esperado, puede llevar a cabo un restablecimiento de fábrica utilizando una memoria USB.

Antes de empezar

- Realice una copia de seguridad de toda la configuración de Security Center con SV Control Panel. Para más información, ver Crear una copia de respaldo de la base de datos de su Directory en la página 33.
- Obtenga una memoria USB con 32 GB de almacenamiento como mínimo. Algunas memorias USB no pueden hacer arrancar la imagen; si sucede esto, intente utilizar otra marca o modelo de memoria.

  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 desea restaurar o instalar.
- Tenga el ID del sistema y la contraseña que se le envió por correo electrónico cuando compró el dispositivo.
- (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

- Para dispositivos con números de modelo distintos de SV-100E, SV-300E y SV-350E, consulte Realizar un restablecimiento de fábrica en un dispositivo Streamvault de estación de trabajo o servidor en la página 78.
- Restablecer a valores de fábrica borra y sobrescribe todos los datos que se encuentran en la unidad de Windows (C:), incluidas las bases de datos y los registros.

Para realizar un restablecimiento de fábrica en un dispositivo de las series SV-100E, SV-300E o SV-350E:

1 Cree una memoria USB de restablecimiento de fábrica que contenga la imagen de software.

2 Con la memoria USB, restablezca la imagen en su dispositivo.

Después de que concluya

Configure su dispositivo.

Temas relacionados

Encontrar la ID de sistema y el número de revisión de software de un dispositivo Streamvault en la página 70

Cómo restablecer la imagen de software en un dispositivo SV-100E, SV-300E o SV-350E con un USB de arranque

Puede restablecer la imagen del software mediante una unidad de recuperación USB.

Antes de empezar

- Tenga la memoria USB que contiene la imagen del software de recuperación para su dispositivo.
- Tenga la licencia correcta para la versión de Security Center desea restaurar o instalar.

- Tenga el ID del sistema y la contraseña que se le envió por correo electrónico cuando compró el dispositivo.

Lo que debería saber

- Restablecer a valores de fábrica borra y sobrescribe todos los datos que se encuentran en la unidad de Windows (C:), incluidas las bases de datos y los registros.

  PRECAUCIÓN: Solo se eliminan los archivos en C :, pero le recomendamos que haga una copia de seguridad de los archivos de video en todas sus unidades.
- El restablecimiento demora alrededor de 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.

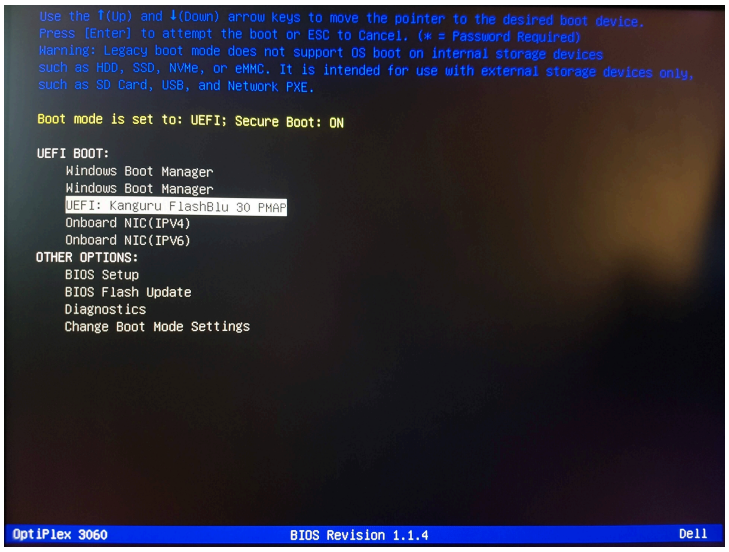
Vea este video para restablecer la imagen del software en un dispositivo SV-100E, SV-300E o SV-350E mediante un USB de arranque.

Para restablecer la imagen del dispositivo de la serie SV-100E, SV-300E o SV-350E:

1 Apague el dispositivo.

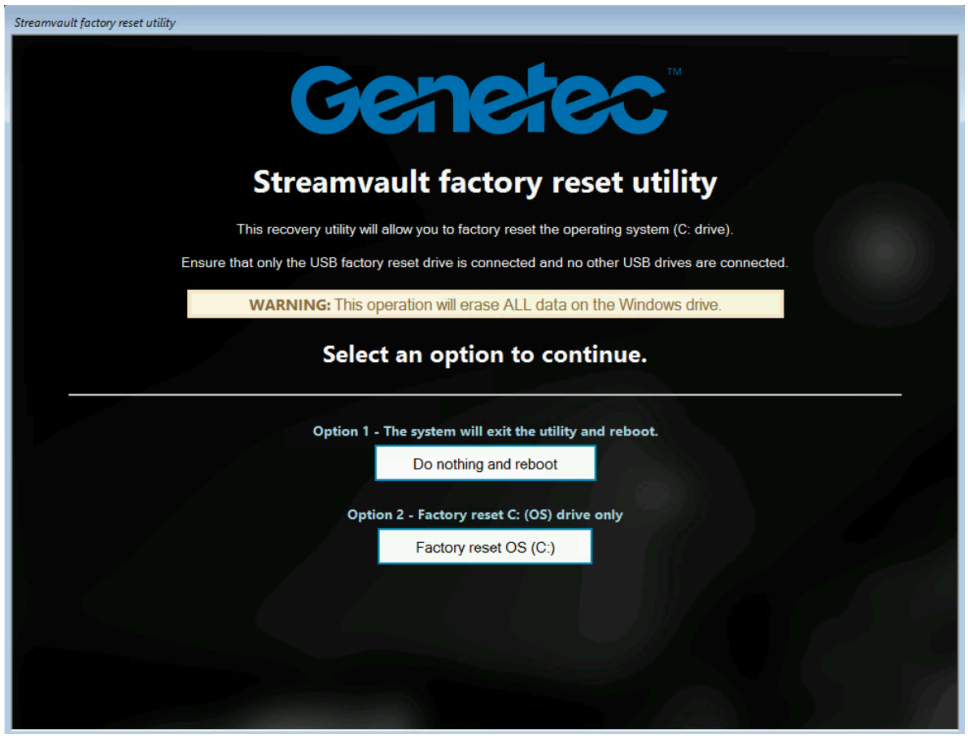
2 Introduzca la memoria USB que creó en un puerto USB.

3 Seleccione la memoria USB y presione Entrar.



4 Cuando la memoria USB arranque en modo de recuperación, seleccione una de las siguientes opciones:

- **No hacer nada y reiniciar:** Elija esta opción para salir del programa de recuperación y reiniciar el dispositivo.
- **Restablecer SO de fábrica (C:):** Elija esta opción para formatear y reinstalar la unidad del sistema del dispositivo y preservar los archivos de video en las demás unidades de video. Todos los archivos que se encuentran en la unidad C: se perderán: registros de bases de datos y demás.



5 Cuando se le solicite, escriba Yes (Sí), pulse Enter para continuar con el restablecimiento de fábrica y espere a que se complete el proceso.

6 Cuando se complete el restablecimiento de fábrica, retire la memoria USB del dispositivo y pulse Entrar para reiniciar.

7 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™.

Puede encontrar estos números en la etiqueta de Genetec ubicada en la parte superior del dispositivo. Si no hay una etiqueta, puede ingresar cualquier texto para continuar.

Aparece el botón **Iniciar**.

8 Haga clic en **Iniciar**.

Se muestra uno de los siguientes mensajes de estado:

- **APROBADO:** El proceso se validó como exitoso. Continúe con el paso siguiente.
- **APROBADO: sin transmisión:** El proceso se validó como exitoso; no obstante, la conexión a Internet no estaba disponible en ese momento. Continúe con el paso siguiente.
- **DESAPROBADO:** El proceso fue validado como fallido. Comuníquese con la asistencia técnica de Genetec.

9 Si recibe un mensaje APROBADO o NO APROBADO: sin transmisión, cierre la ventana del *Validador de Producto de Genetec™*.

10 Espere a que se cierre la secuencia de comandos en segundo plano y luego reinicie el dispositivo.

Después de que concluya

- Inicie sesión en Windows con el nombre de usuario y la contraseña predeterminados que figuran en el adhesivo adherido al dispositivo.

- Activa tu licencia.
- Si realizó una copia de respaldo de la configuración de Security Center antes de llevar a cabo el restablecimiento a valores de fábrica, restaure la configuración a través de SV Control Panel.

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

- Realice una copia de seguridad de toda la configuración de Security Center con SV Control Panel. Para más información, ver Crear una copia de respaldo de la base de datos de su Directory en la página 33.
- Obtenga una memoria USB con 32 GB de almacenamiento como mínimo. Algunas memorias USB no pueden hacer arrancar la imagen; si sucede esto, intente utilizar otra marca o modelo de memoria.

  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 desea restaurar o instalar.
- Tenga el ID del sistema y la contraseña que se le envió por correo electrónico cuando compró el dispositivo.

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 dispositivos integrales, consulte Restablecimiento de fábrica en un dispositivo SV-100E, SV-300E o SV-350E en la página 74.
- 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 cuando las unidades de disco duro, las unidades RAID o las particiones del dispositivo se cambiaron de la configuración predeterminada de fábrica. Si este es el caso, comuníquese con el Centro de Asistencia Técnica de Genetec™ (GTAC, por sus siglas en inglés).

Para realizar un restablecimiento de fábrica en dispositivos Streamvault de estación de trabajo o servidor:

1 Cree una memoria USB de restablecimiento de fábrica.

2 Con la memoria USB, restablezca la imagen en su dispositivo.

Después de que concluya

Configure su dispositivo.

Temas relacionados

Encontrar la ID de sistema y el número de revisión de software de un dispositivo Streamvault en la página 70

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

Puede restablecer la imagen de software de su dispositivo Streamvault a su estado predeterminado utilizando una unidad USB de recuperación.

Antes de empezar

- Asegúrese de tener la memoria USB que contiene el software de recuperación para su dispositivo.

Lo que debería saber

- El restablecimiento borra todos los datos que se encuentran en la unidad del sistema (SO) en ese momento.
- El restablecimiento no afecta los ajustes predeterminados 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 han cambiado desde la configuración predeterminada de fábrica. Si este es el caso, comuníquese con el Centro de Asistencia Técnica de Genetec™ (GTAC, por sus siglas en inglés).

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

Para restablecer la imagen en el Streamvault aparato:

1 Apague el dispositivo.

2 Introduzca la memoria USB de arranque que creó en un puerto USB.

3 Encienda el dispositivo Streamvault.

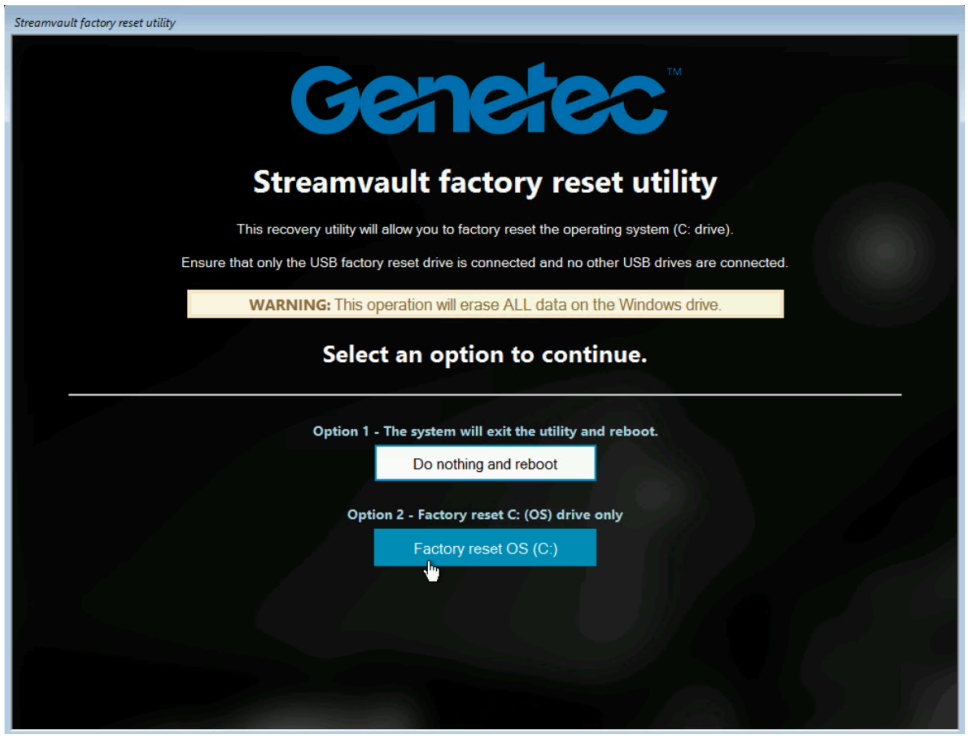
4 Cuando se le solicite, pulse F12.

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. Podría tardar hasta 20 minutos, dependiendo de la velocidad de su memoria USB.

8 Una vez que se complete el restablecimiento a valores de fábrica, cuando se le indique reiniciar la estación de trabajo, presione Entrar.

9 Retire la memoria USB del puerto USB.

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

Después de que concluya

- Inicie sesión en Windows con el nombre de usuario y la contraseña predeterminados que figuran en el adhesivo adherido al dispositivo.
- Activa tu licencia.
- Si realizó una copia de respaldo de la configuración de Security Center antes de llevar a cabo el restablecimiento a valores de fábrica, restaure la configuración a través de SV Control Panel.

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

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

No recibe ningún error o advertencia sobre este problema.

Se aplica a:

- SV-100E 16.3 y versiones posteriores
- SV-300E 16.3 y versiones posteriores
- 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

Habilite TLS 1.1 en el Editor del Registro de Windows.

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 del software Streamvault 16.3 y versiones posteriores.
- TLS 1.0 está deshabilitado en la imagen del software Streamvault 16.0 y versiones posteriores.
- Solo habilite la versión de TLS que requiere su dispositivo.
- Debe habilitar 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. Por este motivo, solo puede habilitar TLS desde el Editor del Registro de Windows.

Para habilitar TLS en un dispositivo:

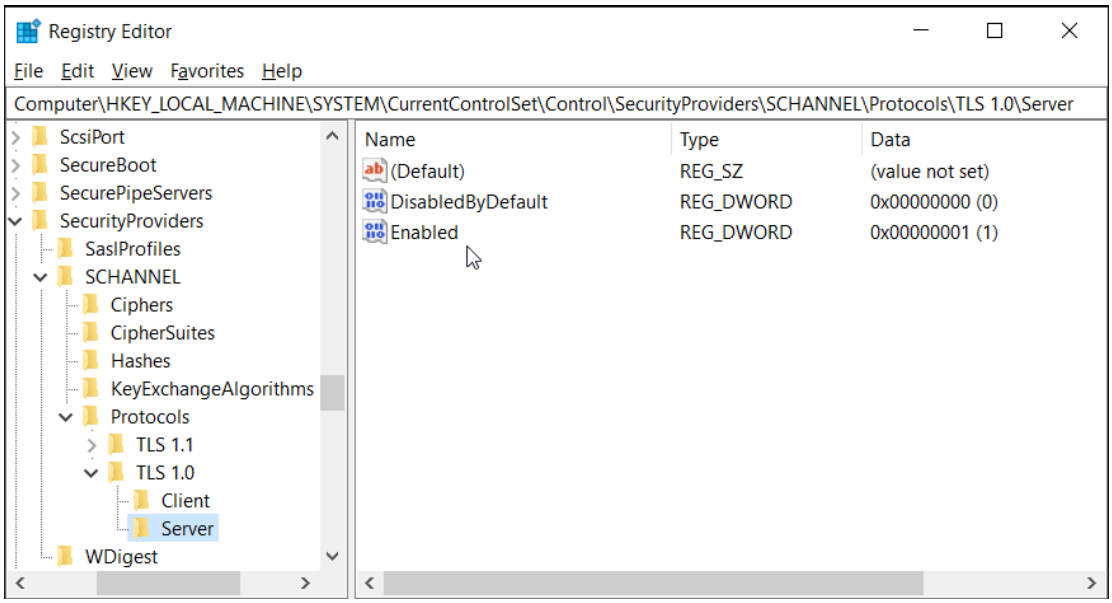
1 Abra el Editor del Registro de Windows.

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.

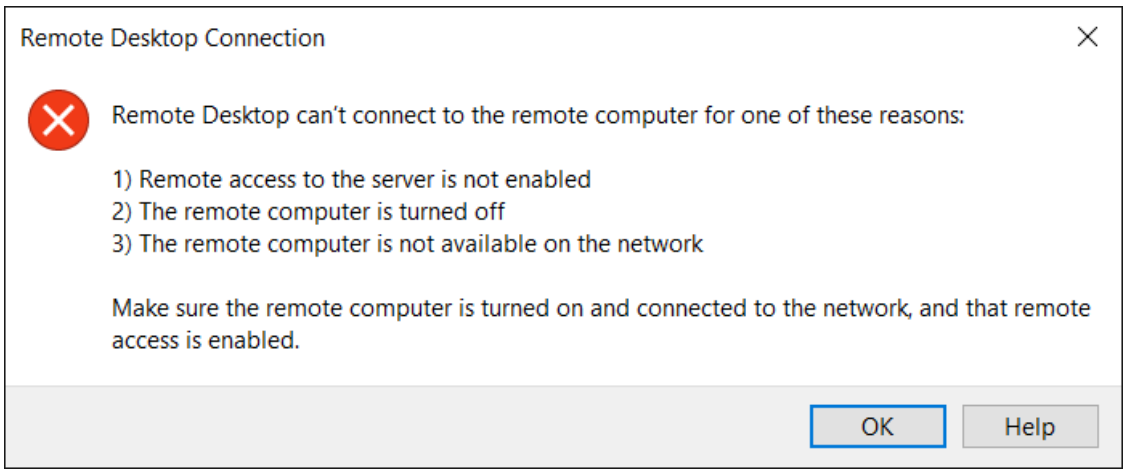
c) Seleccione el nodo de **Cliente**, establezca **DisabledByDefault** en 0 y establezca **Activado** en 1.



3 Reinicie Windows.

El Escritorio Remoto no se puede conectar a un dispositivo Streamvault

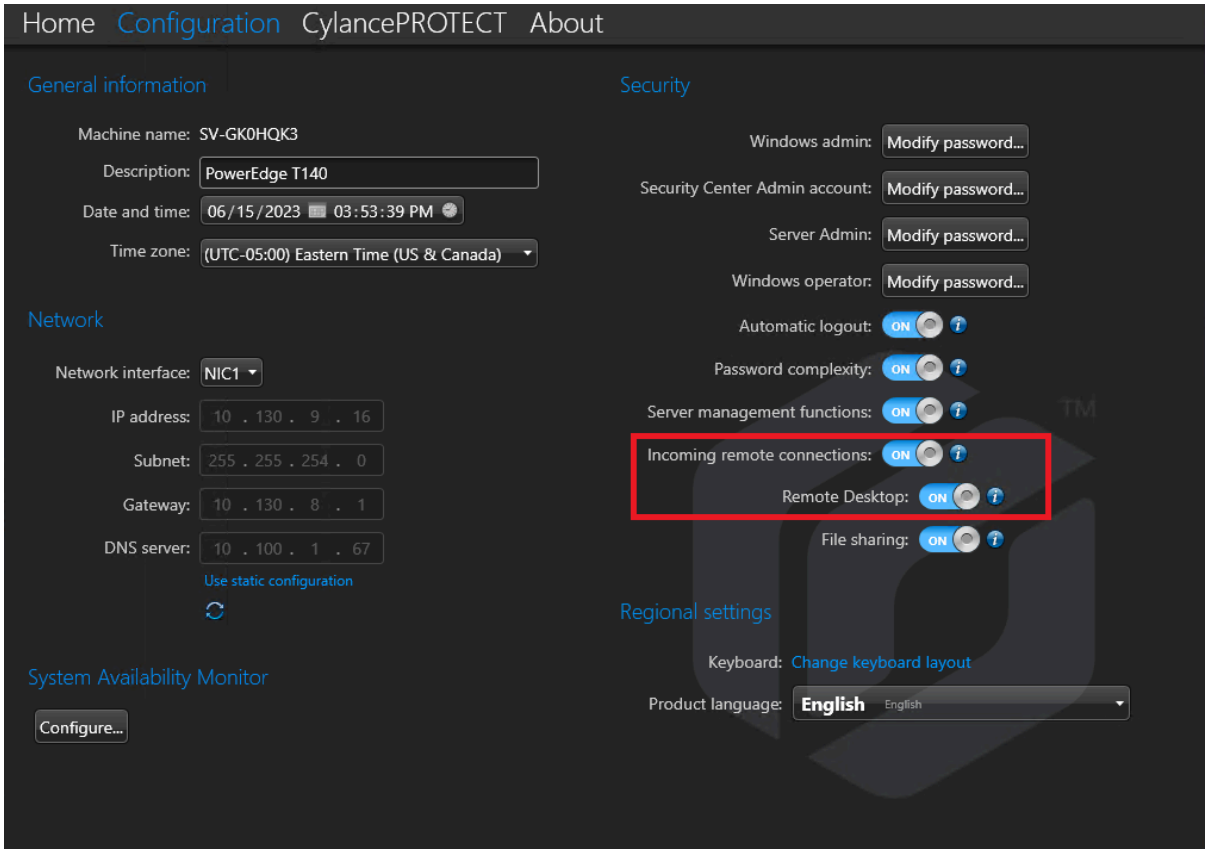
Cuando intenta tener acceso a un dispositivo SV mediante Escritorio remoto, recibe un mensaje que indica que Escritorio remoto no puede conectarse a la computadora remota.



Las conexiones remotas y el Escritorio Remoto están deshabilitados en SV Control Panel

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

Solución: Habilitar el acceso remoto en el dispositivo. En la página *Configuración* de SV Control Panel, habilite **Conexiones remotas entrantes** y **Escritorio Remoto**.



Las conexiones remotas o el escritorio remoto no están permitidos en Windows

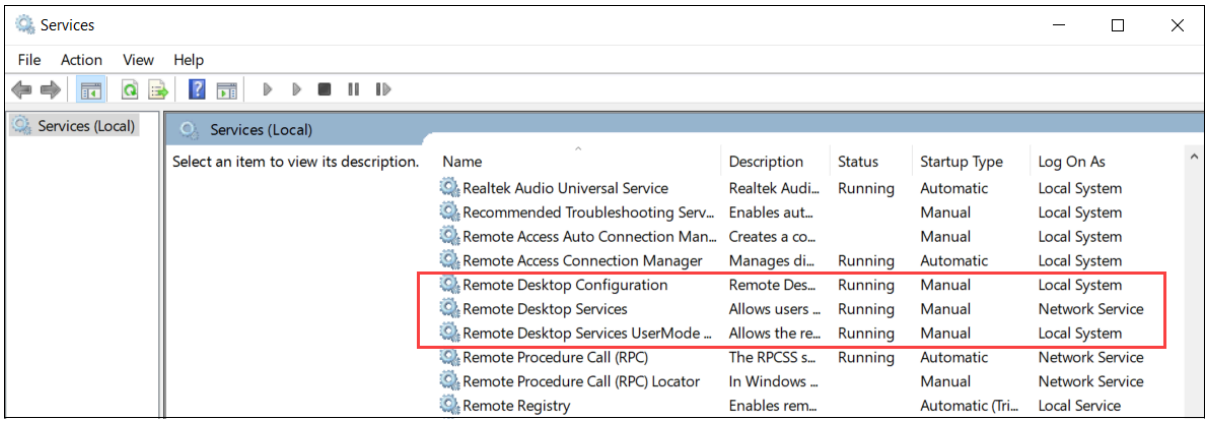
Descripción: Aunque tanto **Conexiones remotas entrantes** como **Escritorio Remoto** están habilitadas en SV Control Panel, estas configuraciones no están permitidas en Windows.

Solución: Sobrescriba la configuración de Windows deshabilitando y volviendo a habilitar las opciones de **Conexiones remotas entrantes** y **Escritorio Remoto** en SV Control Panel.

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.

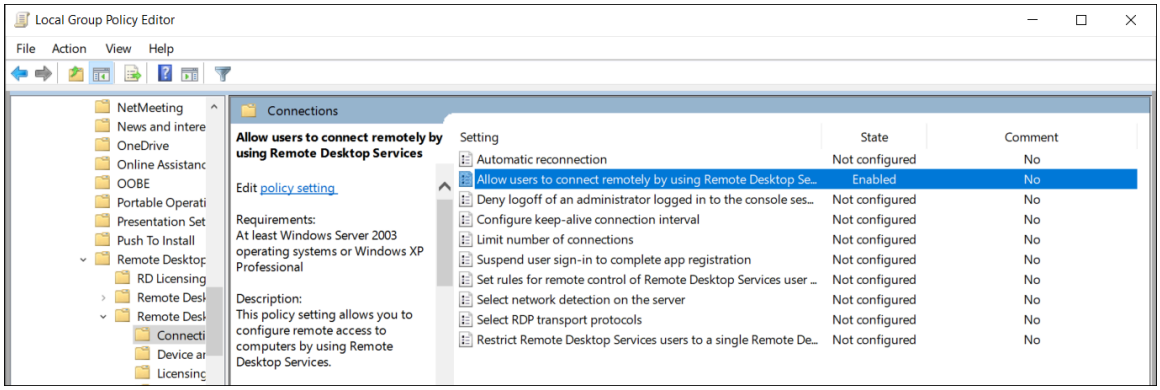


Se deniegan los Servicios de Escritorio Remoto

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

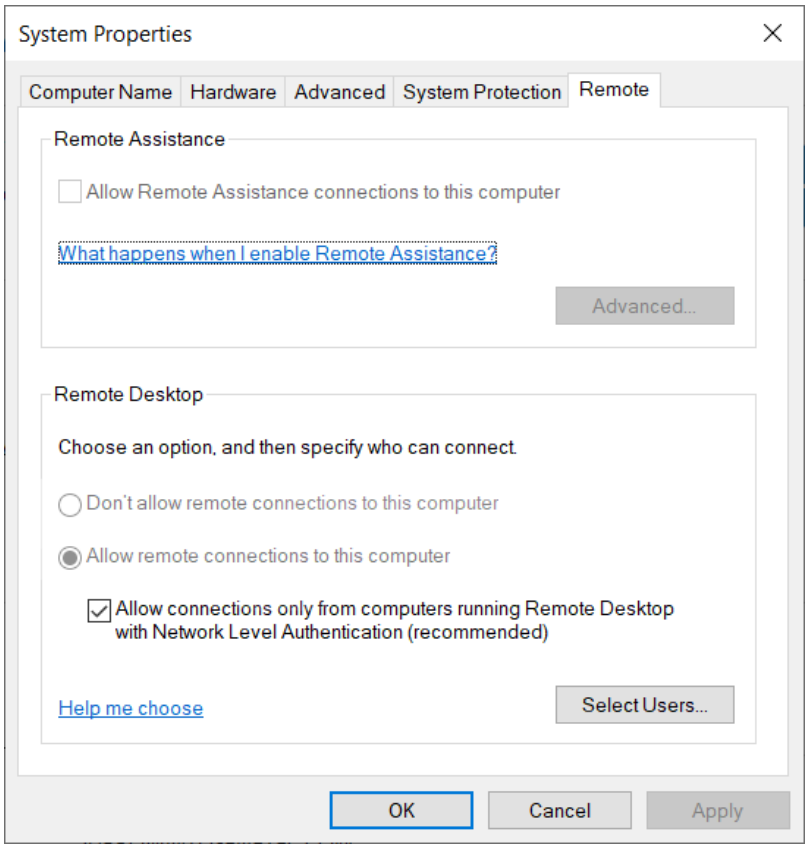
Solución: Permita el acceso de usuarios remotos al dispositivo mediante los Servicios de Escritorio Remoto:

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 /force`.
5. Desde el Panel de Control de Windows, vaya a **Sistema** > **Configuración remota**. Se abre la ventana *Propiedades del Sistema*.

6. En la pestaña *Remoto*, en la sección *Escritorio Remoto*, asegúrese de que la opción **Permitir conexiones remotas a esta computadora** esté seleccionada.



Las directivas de grupo locales 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:

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** > **Asignaciones de Derechos de Usuario**.
3. 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 son compatibles con la autenticación NTLMv2.

NOTA: Si todos los equipos cliente admiten NTLMv2, Microsoft® y varias organizaciones independientes recomiendan la política *Enviar solo respuestas NTLMv2*. Consulte las mejores prácticas y consideraciones de seguridad de Seguridad de red: nivel de autenticación del Administrador de LAN de Microsoft 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 Conexión a Escritorio Remoto aún no puede conectarse, póngase en contacto con el Soporte Técnico.

Temas relacionados

Permitir conexiones a Escritorio Remoto con un dispositivo Streamvault en la página 72

No se puede desinstalar CylancePROTECT de SV Control Panel para algunos dispositivos Streamvault

Apagó la opción **CylancePROTECT** de SV Control Panel, pero CylancePROTECT no se desinstala de tu Streamvault™ dispositivo.

Versiones afectadas

Las siguientes versiones de imágenes de Streamvault se ven afectadas por este problema:

- 0011.2.X.27.G (publicado el 18 de enero de 2021) y posteriores
- 16.8.0 (lanzado el 10 de marzo de 2021) y posteriores
- 2019.1.C.14.G (publicado el 14 de enero de 2021) y posteriores
- 2016.1.C.19.G (publicado el 8 de febrero de 2021) y posteriores

Causa

Un problema de codificación.

Solución alternativa

1. En Windows, abra la consola de *Servicios*.
2. Haga clic derecho en servicio del **Servidor** y haga clic en **Propiedades**.
3. Cambie la opción **Tipo de inicio** a **Manual** y luego inicie el servicio.
4. Abierto SV Control Panel, haga clic en la pestaña **CylancePROTECT** y seleccione la opción **Apagar**.

   Espere 2 minutos para que se complete el proceso.
5. En la consola de *Servicios* en Windows, cambie el **Tipo de inicio** del servicio del **Servidor** a **Desactivado**.
6. Reinicie el dispositivo Streamvault.

7

Soporte técnico

Esta sección incluye los temas siguientes:

Contactar al soporte de Genetec

El Centro de Asistencia Técnica de Genetec™ (GTAC, por sus siglas en inglés) está disponible para ayudarle 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 de asistencia técnica regular. 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 identificación 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 los dispositivos todo en uno). El código es necesario si perdió el acceso administrativo al sistema y necesita una imagen de fábrica.

- Su archivo de registro de diagnóstico TSR (si corresponde).

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

1. Consulte la página Centro de Asistencia Técnica de Genetec *Contacto* para encontrar el número de teléfono de GTAC y el horario comercial en su región.
2. Llame al número de teléfono del Centro de Asistencia Técnica de Genetec y elija la Opción n.° 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, por sus siglas en inglés) a través de chat en vivo y casos de soporte. El horario de atención es de lunes a viernes de 8 a. m. a 8 p. m. (hora local).

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

1. Llame al número de GTAC correspondiente a 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.
5. 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).

Contactar al soporte de Genetec a través de GTAP

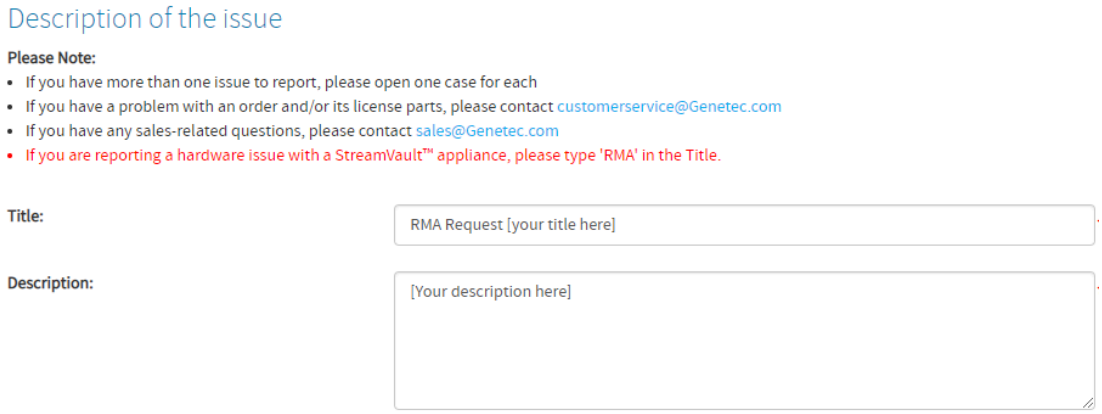
Todos los clientes tienen soporte disponible durante el horario comercial de su región a través de casos de soporte en línea en el Portal de Asistencia Técnica de Genetec™ (GTAP, por sus siglas en inglés).

Para clientes sin cobertura 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 enviar un caso a través del portal en línea:

1. Navegue hasta el Portal de Asistencia Técnica de Genetec.
2. Inicie sesión con su correo electrónico corporativo.
3. Haga clic en **+ Crear Caso**.

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



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

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

Contactar al soporte de Genetec a través del chat en vivo

Los clientes con cobertura Genetec Advantage tienen soporte en vivo disponible durante el horario comercial de su región a través del chat en vivo en el Portal de Asistencia Técnica de Genetec (GTAP, por sus siglas en inglés).

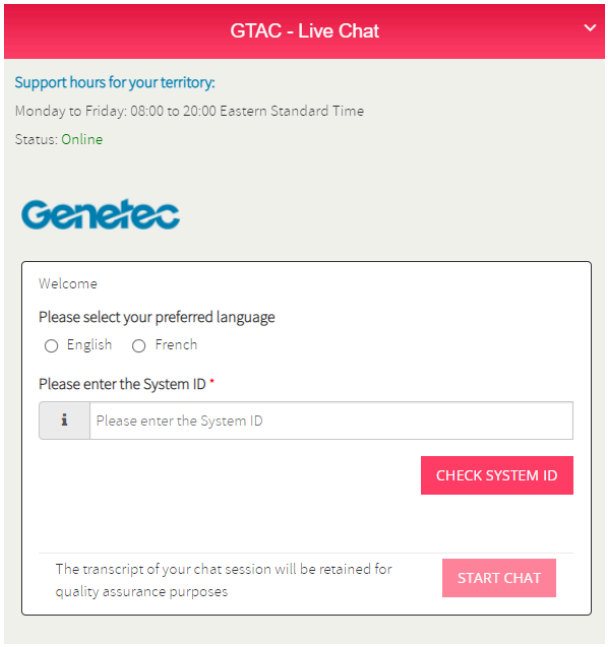
Para clientes sin cobertura Advantage, se debe abrir un caso a través de Portal de Asistencia Técnica de Genetec (GTAP). Para obtener más información sobre Genetec Advantage, comuníquese con advantage@genetec.com.

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 el ID del sistema completo (`GSC-xxxxxx-xxxxxx`) y luego haga clic en **Verificar ID del Sistema**.
6. Elija si desea chatear sobre un caso nuevo o existente.
7. Seleccione el producto.
8. Haga clic en **Iniciar chat**.



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

Software Streamvault™

- La imagen de Windows de Streamvault™ está cubierta por la garantía 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 necesarios, el endurecimiento y el software instalado 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 de Security Center

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 los documentos de Genetec Lifecycle Management (GLM): Descripción de Genetec Advantage y Descripción de Genetec Assurance.

Soporte de hardware

Las garantías de HP y Dell ProSupport están disponibles a través de Genetec. Para cualquier problema de hardware, el Centro de Asistencia Técnica de Genetec (GTAC, por sus siglas en inglés) es su punto de contacto para diagnosticar el problema y coordinar con HP y DellProSupport.

Familia de productos	Duración de la garantía[1]		Reemplazo avanzado o reparación en el sitio	Devolución y reparación en garantía[2]
	Estándar	Extendido		
SV-100E SV-300E SV-350E	3 años	2 años	1 año de repuesto anticipado	Incluido
SVW-300 SVW-500 SV-1000	3 años	No aplica	Garantía de reparación in situ de HP[3]	Incluido
SV-2000E SV-4000E SV-7000E	5 años	2 años	Soporte profesional de Dell siguiente día de negocios[4] Garantía de reparación in situ con conservación de su disco duro.[3]	Incluido
SVW-300E SVW-500E SV-1000E	5 años	No aplica	Soporte profesional de Dell siguiente día de negocios[4] Garantía de reparación in situ con conservación de su disco duro.[3]	Incluido
SV-2000 SV-4000 SV-7000	5 años	2 años	Garantía de reparación in situ de HP[3]	Incluido
Área de Almacenamiento Red (SAN)	5 años	Se puede extender a petición de acuerdo con cada caso en particular.	Soporte profesional de Dell siguiente día de negocios[4] Garantía de reparación in situ con conservación de su disco duro.[3]	Incluido

[1]Puede adquirir una extensión de garantía adicional de 2 años (para un total de 7 años de garantía). Debe adquirirse antes de que se cumplan los 5 años.

[2] Puede optar por devolver la unidad para su reparación o recibir servicios en el sitio.

[3]Para obtener más información sobre los términos definidos por estos proveedores, consulte la documentación de Dell ProSupport y Soporte de HP.

[4]La garantía de reparación en el sitio al siguiente día hábil comienza cuando se completa la resolución de problemas, se identifica el problema de hardware, se presenta el caso a Dell y Dell considera que el problema es una falla de hardware. El siguiente día hábil no se aplica tan pronto como se abre el caso de soporte con Genetec Inc.

Especificaciones para Streamvault™

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

Especificaciones técnicas, mecánicas y medioambientales

Dispositivos todo en uno:

- Hoja de datos del SV-100E
- Hoja de datos del SV-300E
- Hoja de datos del SV-350E

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
- Hoja de datos de la serie NAS SVS-7000E
- Hoja de datos de la serie SAN SVS-7000E

Estaciones de trabajo:

- Hoja de datos de la serie SVW-300E
- Hoja de datos de la serie SVW-500E

Dispositivos preparados para análisis:

- Hoja de datos de la serie SVA-100E
- Hoja de datos de la serie SVA-1000E

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 Extendida de Genetec™ se rigen por los siguientes términos y condiciones con respecto a las reparaciones, los repuestos, los recursos o las exclusiones de la garantía.

Términos y condiciones

Garantía sobre reparaciones y piezas de repuesto

Todos los productos de Genetec™ para los que Genetec Inc. ofrece servicios de reparación y piezas de repuesto están garantizados contra defectos en la fabricación y los materiales por 90 días o el plazo restante de la garantía original, el que sea más extenso. Se pueden aplicar cargos adicionales si el daño surge como consecuencia de usar el producto de un modo distinto de su aplicación habitual.

Para Streamvault™, cualquier equipo reemplazado (o partes de este) pasará a ser propiedad de Genetec Inc. una vez que el Cliente reciba el reemplazo correspondiente, y el cliente deberá devolver de manera oportuna dicho equipo reemplazado (o partes de este) a pedido de Genetec Inc. Si dicho equipo reemplazado no se devuelve dentro de los 30 días posteriores a la recepción de las piezas nuevas, el cliente estará obligado a pagar a Genetec Inc. el valor de la pieza de reemplazo. Esto no se aplica al servicio **Conservación de su Disco Duro**.

Recurso de garantía exclusivo

Durante el período de garantía aplicable y en el caso de que Genetec Inc. determine que un producto tiene defectos de materiales o ensamblaje, Genetec Inc., a su exclusivo criterio, realizará una de las siguientes acciones:

- Acreditar al cliente el precio pagado por el producto defectuoso.
- Reparar el producto defectuoso.
- Reemplazar el producto defectuoso con un producto nuevo o reacondicionado.
- Reemplazar el producto defectuoso con un producto diferente que tenga especificaciones idénticas o mejores

Exclusiones de garantía

Los siguientes artículos no están cubiertos por la Garantía Estándar de Hardware de Genetec:

- Equipos no comprados a Genetec Inc.
- Productos usados con software o equipos auxiliares no compatibles
- Defectos o daños por uso indebido (incluido, entre otros, el uso no conforme con la documentación y los manuales adjuntos), modificaciones indebidas, accidentes o negligencia.
- Defectos o daños por taladrar orificios, agregar calcomanías o adhesivos o pintar el producto.
- Defectos o daños a raíz de daños por agua, rayos, explosiones u otras descargas eléctricas.
- Productos que se desmontan o reparan de una manera que tenga un efecto negativo sobre el rendimiento o impida una inspección y prueba adecuadas para verificar cualquier reclamo de garantía.
- Modificación, abuso o alteración del producto.
- Hechos fortuitos (inundaciones, terremotos, rayos, incendios, fugas de gas, etc.).
- Uso y desgaste normales.

Términos y condiciones de la autorización para la devolución de mercancía de Genetec

Autorización para la devolución de mercancía

Antes de devolver un artículo, el cliente debe obtener un formulario de autorización de devolución de mercancía (RMA, por sus siglas en inglés) de Genetec Inc. El número de RMA debe estar marcado con

claridad en el exterior de cada paquete devuelto y en el formulario de RMA incluido con el paquete. El cliente debe garantizar la devolución del material exacto, en la cantidad correcta y con los números de serie exactos (si corresponde) aprobados por Genetec Inc. y registrados en el formulario de RMA proporcionado. Cualquier inventario no aprobado, mal etiquetado o en exceso que se envíe a Genetec Inc. se rechazará y devolverá al remitente.

Empaque

El cliente es responsable del empaque adecuado de los productos devueltos. Todo daño incurrido durante el transporte debido a un mal empaque no estará cubierto en función de la política de la Garantía de Hardware de Genetec. El cliente es responsable de cualquier daño ocasionado durante el transporte. El incumplimiento resulta en que Genetec Inc. anule la RMA y se cobren las tarifas de reparación o el costo total de reemplazo.

Flete

El cliente es responsable de todos los costos incurridos para devolver la unidad. A menos que se anule la RMA, Genetec Inc. es responsable de todos los costos incurridos para devolver los productos reparados o las unidades de reemplazo al cliente.

Si Genetec Inc. envía productos no comprados o un excedente de productos al cliente por error, Genetec Inc. cubre los costos de devolver los productos proporcionando al cliente etiquetas de envío y documentos de exportación, en caso de ser necesario. Si no lo hace, se envía una factura al cliente por los productos.

En determinadas circunstancias, Genetec Inc. acepta la devolución de artículos no dañados y emite un crédito. Para ser elegible para una devolución por crédito, el artículo debe estar sin usar y en las mismas condiciones en las que se recibió. Asimismo, debe estar en el empaque original. El artículo debe devolverse en un plazo de 30 días a partir de la fecha en que se envió al cliente o dentro del período permitido por el proveedor de Genetec Inc., el que sea más corto.

Para todas las devoluciones por crédito, Genetec Inc. emite un crédito una vez que los productos se hayan recibido, inspeccionado y encontrado en su estado original. El crédito se emite por el precio de venta original menos la tarifa de reposición aplicable según el Anexo A. Genetec Inc. se reserva el derecho de rechazar cualquier devolución por crédito. Asimismo, Genetec Inc. se reserva el derecho de modificar el cargo de reabastecimiento en circunstancias inusuales, según el exclusivo criterio de Genetec Inc.

Los artículos personalizados vendidos bajo una política no cancelable ni reembolsable (NCNR, por sus siglas en inglés) no son elegibles para una devolución por crédito.

Daños en el envío

Los productos deben inspeccionarse una vez recibidos. Todo daño producido durante el envío debe informarse a Genetec Inc. en un plazo de 14 días desde la recepción del producto. Si no se informan los daños en un plazo de 14 días desde su recepción, Genetec Inc. se reserva el derecho de denegar una devolución por crédito o el reemplazo de los productos dañados. Para productos dañados durante el envío, envíe un correo electrónico customerservice@genetec.com de inmediato. Se requiere una descripción de los daños, con fotografías si es posible.

Responsabilidades y expectativas

- Las RMA son válidas por 30 días. Los artículos deben ser devueltos dentro de este plazo e identificados con el número de RMA correspondiente.
- Para devoluciones en las que el cliente elige omitir el Centro de Asistencia Técnica de Genetec (GTAC, por sus siglas en inglés), el cliente está obligado a pagar un cargo de inspección si no se encuentra ningún defecto en las unidades devueltas de acuerdo con el Anexo A.
- Las unidades enviadas al cliente como parte de la garantía de “reemplazo avanzado” se facturan al cliente de inmediato y se acreditan si la unidad dañada se devuelve dentro de los 30 días posteriores a la fecha de creación de RMA.
- El cliente es responsable de devolver las unidades en buenas condiciones y de acuerdo con las instrucciones proporcionadas en este documento. El incumplimiento por parte del cliente puede dar lugar a cargos adicionales para el cliente o a que Genetec Inc. anule la Solicitud de RMA.

- Si se considera que una unidad de repuesto anticipado ha sido manipulada de forma indebida, abusada o utilizada para fines distintos a los previstos, se le puede cobrar al cliente el precio total de la unidad de repuesto anticipado en virtud de la garantía de “repuesto anticipado”.
- Las devoluciones y reparaciones fuera de garantía se cobran según el Anexo A.

Instrucciones de devolución

1. Reúna los siguientes detalles antes de comunicarse con Genetec Inc. para obtener una RMA:
   - Nombre de la empresa (integrador) que realizó la orden.
   - Número de orden del cliente (número de orden de compra) para la unidad que requiere una RMA.
   - Información de contacto válida (nombre, dirección de correo electrónico, número de teléfono) para futura correspondencia.
   - El número de pieza de la unidad que necesita reparación, repuesto o crédito.
   - El número de serie de la unidad que requiere una RMA, según corresponda.
   - La identificación del sistema, en caso de estar disponible.
   - Motivo de la devolución.
   - Tantos detalles como sea posible sobre el problema de hardware, si corresponde.
2. Comuníquese con Genetec Inc. para solicitar una RMA.

RMA de devolución y reparación

1. Comuníquese con el Centro de Asistencia Técnica de Genetec (GTAC, por sus siglas en inglés) para informarnos sobre el problema y solicitar una RMA.

   Para los clientes con cobertura Genetec Advantage, el soporte en vivo está disponible durante el horario comercial por teléfono y a través de nuestros servicios de chat en línea en el Portal de Asistencia Técnica de Genetec (GTAP, por sus siglas en inglés). Para los clientes sin cobertura Advantage, se debe abrir un caso a través de GTAP. Al crear el caso, incluya **Solicitud de RMA** en el título para que nuestro equipo pueda identificar con facilidad estas solicitudes. 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*.
2. El Servicio de Atención al Cliente de Genetec proporciona al cliente un formulario RMA.

   Este formulario es necesario para devolver la unidad. El cliente recibe el formulario por correo electrónico dentro de las 24 horas siguientes al contacto con GTAC y su procesamiento por parte del Servicio al Cliente. Este formulario de RMA otorga al cliente la dirección de devolución completa para Genetec Inc. o el proveedor, y el número de RMA de Genetec Inc. o el proveedor.

RMA de devolución por crédito

1. Comuníquese con el Servicio al Cliente de Genetec para informarnos el motivo de la devolución. La solicitud se puede presentar enviando un correo electrónico a customerservice@genetec.com, o por teléfono. Para encontrar el número de teléfono del Servicio al Cliente y el horario comercial de su región, consulte la página de *Contáctenos* en el sitio web de Genetec Inc.
2. El Servicio de Atención al Cliente de Genetec proporciona al cliente un formulario RMA.

   Este formulario es necesario para devolver la unidad. El cliente recibe el formulario por correo electrónico en un plazo de 24 horas a partir del contacto con el Servicio al Cliente de Genetec. Este formulario de RMA proporciona al cliente la dirección de devolución completa y el número de RMA de Genetec Inc. o del proveedor.

3. El cliente devuelve la unidad a Genetec Inc. o al proveedor.
   a. El cliente es responsable de todos los gastos de envío relacionados con la devolución del producto a Genetec Inc. o al proveedor correspondiente.
   b. El cliente debe imprimir el formulario de RMA (enviado por correo electrónico por Genetec Inc. al cliente) e incluirlo en el paquete, junto con la unidad, para que Genetec Inc. o sus proveedores identifiquen el paquete.
   c. El número de RMA debe estar a la vista en el exterior del paquete. Genetec Inc. proporciona este número al cliente en el formulario de RMA.
   d. El cliente debe enviar solo los productos para los cuales se solicitó la RMA. Debe enviarlos a la dirección completa que se proporciona en el formulario de RMA.
   e. Genetec Inc. o el proveedor deben recibir la unidad devuelta en un plazo de 30 días a partir de la emisión de la RMA. Después de este plazo de 30 días, se anulará toda RMA para servicios de "Devolución por crédito" o "Devolución y reparación".
   f. Para servicios de "reemplazo avanzado", Genetec Inc. envía la unidad de reemplazo cuando se crea la RMA o cuando la pieza esté disponible.

      NOTA: Si la unidad dañada se devuelve dentro de los 30 días posteriores a la fecha de creación de RMA, las unidades enviadas al cliente como parte de la garantía de "reemplazo avanzado" se facturan al cliente de inmediato y se acreditan.
   g. Genetec Inc. requiere que el cliente envíe un número de seguimiento por correo electrónico a Servicio al Cliente.
4. Genetec Inc. recibe e inspecciona los artículos devueltos.
   a. El número de pieza y el número de serie (si corresponde) de la unidad devuelta deben coincidir con la información que el cliente proporcionó a Genetec Inc. cuando se creó la RMA. Si hay discrepancias, el Servicio al Cliente de Genetec se comunica con el cliente. La RMA no se procesará hasta que el cliente haya sido contactado, ya que la garantía puede variar según el número de serie y el número de pieza.
   b. **Devolución por crédito**: Si no está dañada, la unidad se procesa como una "devolución por crédito". Solo se aplica un crédito cuando se haya recibido e inspeccionado la unidad. Si el empaque está dañado o modificado de alguna manera, Genetec Inc. tiene el derecho de denegar el crédito. Se cobra una tarifa de reposición por una "devolución por crédito" según el Anexo A.
   c. **Devolución para reparación**: Si está dentro de la garantía y no se considera que el daño de la unidad sea consecuencia de un abuso o manipulación indebida por parte del cliente, Genetec Inc. o el proveedor proceden con la reparación. Luego, la unidad reparada se devuelve al cliente. En los casos en que la reparación no sea posible, el producto podría reemplazarse por un producto con funcionalidad completa, ya sea reacondicionado o nuevo, según disponibilidad. Los plazos de reparación varían en función de la línea de productos, el tipo de producto, la cantidad y el fabricante. Si no está en garantía, o si la RMA se anula, Genetec Inc. determina si el artículo es reparable. En tales casos, los costos de reparación se aplican según el Anexo A.
   d. Repuesto anticipado: Si la unidad devuelta está cubierta por una cláusula de "repuesto anticipado", y no se considera que el daño de la unidad sea consecuencia de un abuso o manipulación indebida por parte del cliente, no se cobra cargo alguno al cliente por la unidad de repuesto provista por Genetec Inc.
5. Genetec Inc. procesa la RMA y devuelve la unidad según corresponda.

   Genetec Inc. es responsable de todos los gastos de envío y las tarifas aduaneras (según corresponda) por devolver la unidad al cliente.

   El número de seguimiento se comunica al cliente por correo electrónico cuando se envía el artículo.

Anexo A

Familia de productos	Tarifas de reposición	Tarifas de reparación[3]	Tarifas de inspección
Streamvault	Las tarifas se evalúan caso por caso y se comunican al cliente.	Las tarifas se evalúan caso por caso y se comunican al cliente.	No aplica

[3]Si la unidad no se puede reparar, se le informa al cliente que determine si desea continuar con un reemplazo de la unidad.

Glosario

Administrador de Streamvault™

La entidad Streamvault™ manager se usa para controlar las configuraciones de alertas para un grupo de entidades de monitor de hardware de Streamvault™. Solo se admite un Streamvault™ manager 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 de Streamvault™ es una tarea de informes de Security Center que puede usar para ver una lista de problemas de salud que afecten a sus dispositivos Streamvault™.

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 necesita un monitor de Hardware de Streamvault™ por dispositivo de Streamvault™.

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. SV-1000E viene con Security Center y SV Control Panel 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. SV-2000E viene con Security Center y SV Control Panel 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 el almacenamiento de videos críticos.

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. SV-4000E viene con Security Center y SV Control Panel 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. SV-7000E viene con Security Center y SV Control Panel 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 analíticos 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. 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. 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. Para tener acceso al TechDoc Hub, inicie sesión en el Portal de Genetec y haga clic en TechDoc Hub. ¿No encuentra lo que busca? 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.