Shavlik Protect

Guía de actualización

shavlik

Copyright

Marcas comerciales

Información del documento e historial de ediciones

Número de documento: N/D

Fecha	Versión	Descripción
Septiembre de 2010	NetChk Protect 7.6	Actualizada la marca del producto, agregada información sobre la nuevas funciones y mejoras de la versión 7.6.
Marzo de 2011	NetChk Protect 7.8	Agregada información acerca de la nuevas funciones y mejoras de la versión 7.8.
Octubre de 2011	VMware vCenter Protect 8.0	Actualizada la marca del producto, agregada información sobre las tareas de actualización a la versión 8.0. Eliminada toda la información sobre las versiones anteriores a 7.5.
Diciembre de 2011	VMware vCenter Protect 8.0, revisión A del documento	Agregado paso que explica cómo comprimir la base de datos antes de comenzar el proceso de actualización.
Septiembre de 2012	VMware vCenter Protect 8.0.1	Actualizados el nombre y la versión del producto, actualizados los gráficos de la portada.
Mayo de 2012	Shavlik Protect 9.0	Actualizados los requisitos del sistema. Agregada información sobre la nuevas funciones y mejoras de la versión 9.0.
Abril de 2014	Shavlik Protect 9.1	Actualizados los requisitos del sistema. Agregada información sobre la nuevas funciones y mejoras de la versión 9.1.
Septiembre de 2015	Shavlik Protect 9.2	Actualizados los requisitos del sistema. Agregada información sobre la nuevas funciones y mejoras de la versión 9.2.

BIENVENIDO

Propósito de esta guía

Bienvenido a Shavlik Protect 9.2. En este documento se describe cómo actualizar Shavlik Protect 9.0 o Shavlik Protect 9.1 a Shavlik Protect 9.2.

Además de describir el procedimiento de actualización, este documento enumera una serie de diferencias funcionales que debe conocer al realizar la actualización a Shavlik Protect 9.2. también destaca qué áreas de la interfaz de usuario han cambiado significativamente.

Nuevos requisitos del sistema y prerrequisitos

Tenga en cuenta los siguientes requisitos y prerrequisitos nuevos de la consola de Shavlik Protect 9.2.

- Windows 2000 ya no es un sistema operativo compatible en los equipos clientes.
- Windows 10 (Pro o Enterprise Editions) ahora es compatible en equipos clientes.

Los prerrequisitos de software ausentes se instalarán automáticamente durante el proceso de actualización. Para obtener la lista completa de los requisitos del sistema, consulte *Shavlik Protect Installation Guide* (Guía de instalación de Shavlik Protect).

Requisitos de la cuenta de usuario para la actualización

Para realizar la actualización, la cuenta de usuario debe cumplir los requisitos siguientes:

- El usuario que actualice la base de datos debe ser miembro del rol db_owner.
- Si tiene varias consolas que comparten una base de datos y enlazan una consola adicional con una base de datos ya actualizada, la cuenta del usuario que utilice debe ser miembro de los siguientes roles de la base de datos: db_datareader, db_datawriter, STExec y STCatalogupdate. Además, la cuenta de servicio utilizada para las operaciones en segundo plano también debe ser miembro del rol db_owner. Si su cuenta es un miembro de los roles b_securityadmin y db_accessAdmin, la herramienta de actualización de la base de datos intentará automáticamente asignarle y configurar los roles necesarios.

PROCEDIMIENTO DE ACTUALIZACIÓN

Resumen

En esta sección se describe cómo actualizar Shavlik Protect 9.0 o Shavlik Protect 9.1 a Shavlik Protect 9.2. Si va a aprovechar la oportunidad para mover la consola a un equipo nuevo y desea realizar la migración utilizando la herramienta de migración, consulte *Shavlik Protect Migration Tool User's Guide* (Guía de usuario de la herramienta de migración de Shavlik Protect) antes de proceder.

Antes de realizar la actualización, lea la sección Cambios y mejoras significativos en la página 18 para saber cómo afecta la actualización al sistema. También puede tomar nota de los ajustes actuales del usuario personalizado, ya que algunos no se mantienen después de las actualizaciones (consulte la página 17).

Realizar la actualización

1. Comprima la base de datos utilizada para almacenar los resultados de los análisis, de los despliegues de parches y de las medidas correctoras de amenazas.

   Puede hacerlo en SQL Server Management Studio haciendo clic con el botón derecho en la base de datos ShavlikScans y seleccionando **Tareas** > **Reducir** > **Base de datos**.

2. Cree una copia de seguridad de la base de datos actual con SQL Server Management Studio.
3. Cierre todos los programas que se estén ejecutando en el equipo de la consola, incluido Shavlik Protect.
4. Descargue el archivo ejecutable de Shavlik Protect 9.2 en el equipo de la consola utilizando el siguiente vínculo:

   http://www.shavlik.com/downloads/

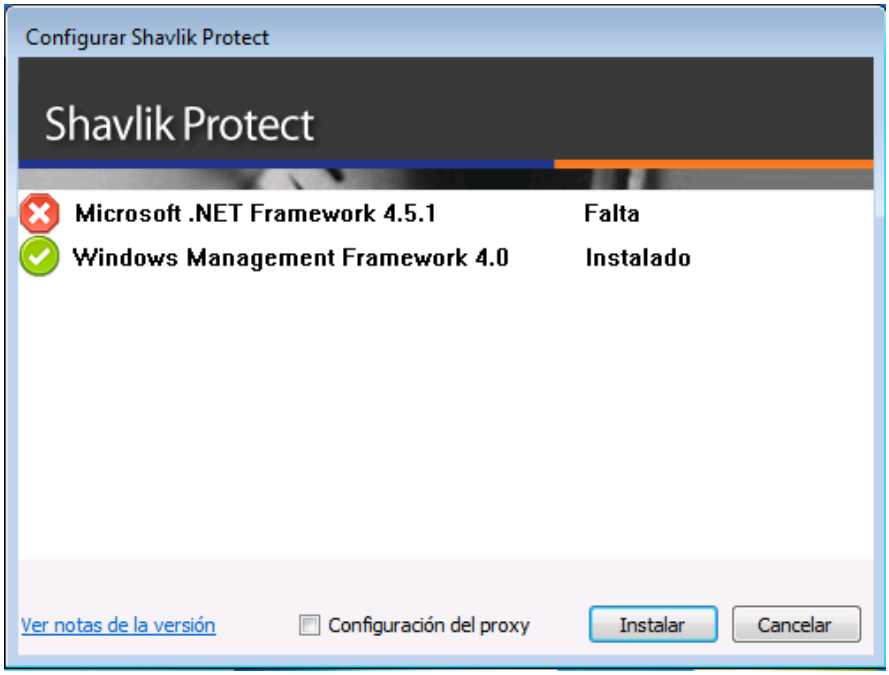
5. Comience el proceso de instalación mediante uno de los métodos siguientes:
   - Haga doble clic en el archivo denominado **ShavlikProtect.exe.**
   - Escribir el nombre de archivo en el símbolo del sistema. De esta forma puede utilizar una o varias opciones de líneas de comando. Contemple la posibilidad de utilizar este método si se actualiza una base de datos de gran tamaño. La opción DBCOMMANDTIMEOUT se utiliza para especificar el valor del tiempo de espera del comando SQL durante la instalación. El valor predeterminado es 15 minutos por GB. El valor mínimo del tiempo de espera es el mayor de 15 minutos por GB o 1800 segundos (30 minutos). Si la base de datos es de 4 GB, aumente el valor a 3600 segundos (60 minutos). Por ejemplo:

     ```
     ShavlikProtect /wi:"DBCOMMANDTIMEOUT =3600"
     ```

Nota: Si recibe un aviso que le indique que es necesario reiniciar, haga clic en **Aceptar** y el proceso de instalación continuará automáticamente después del reinicio.

6. Conteste al diálogo que pregunta si desea continuar con la actualización.

   Si hace clic en Sí y al equipo de la consola le faltan uno o más prerrequisitos, aparecerá un cuadro de diálogo similar al siguiente. Si no faltan prerrequisitos, omita el paso siguiente y vaya al diálogo Bienvenida.



7. Haga clic en **Instalar** para instalar los prerrequisitos ausentes.

   Es posible que el Asistente de instalación necesite llevar a cabo un reinicio durante esta parte del proceso de instalación. Cuando el equipo se reinicia aparece el diálogo Configuración. Haga clic en Instalar para continuar con la instalación.

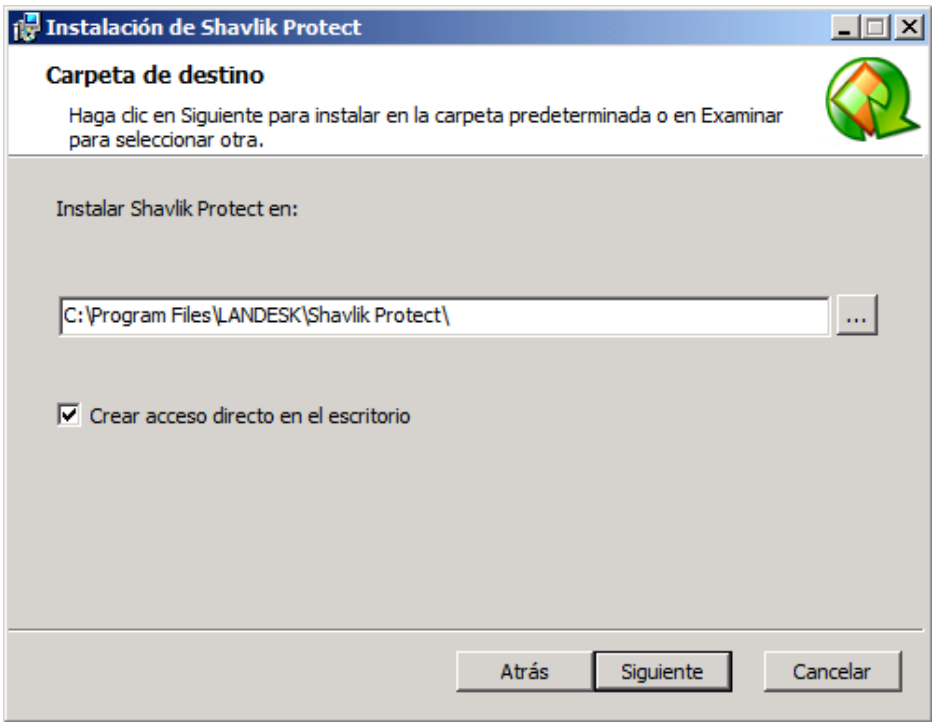
   Aparece el cuadro de diálogo **Bienvenido.**

8. Lea la información que aparece en el cuadro de diálogo **Bienvenido** y a continuación, haga clic en **Siguiente**.

   Aparece el contrato de licencia. Para instalar el programa debe aceptar los términos del contrato de licencia.

9. Marque la casilla **Acepto los términos del Contrato de licencia** y haga clic en **Siguiente.**

   Aparece el cuadro de diálogo **Carpeta de destino**.



10. Si desea cambiar la ubicación predeterminada del programa, haga clic en el botón Examinar y elija la nueva ubicación. Aquí también tiene la opción de instalar el icono de acceso directo en el escritorio. Cuando haya terminado, haga clic en **Siguiente**.

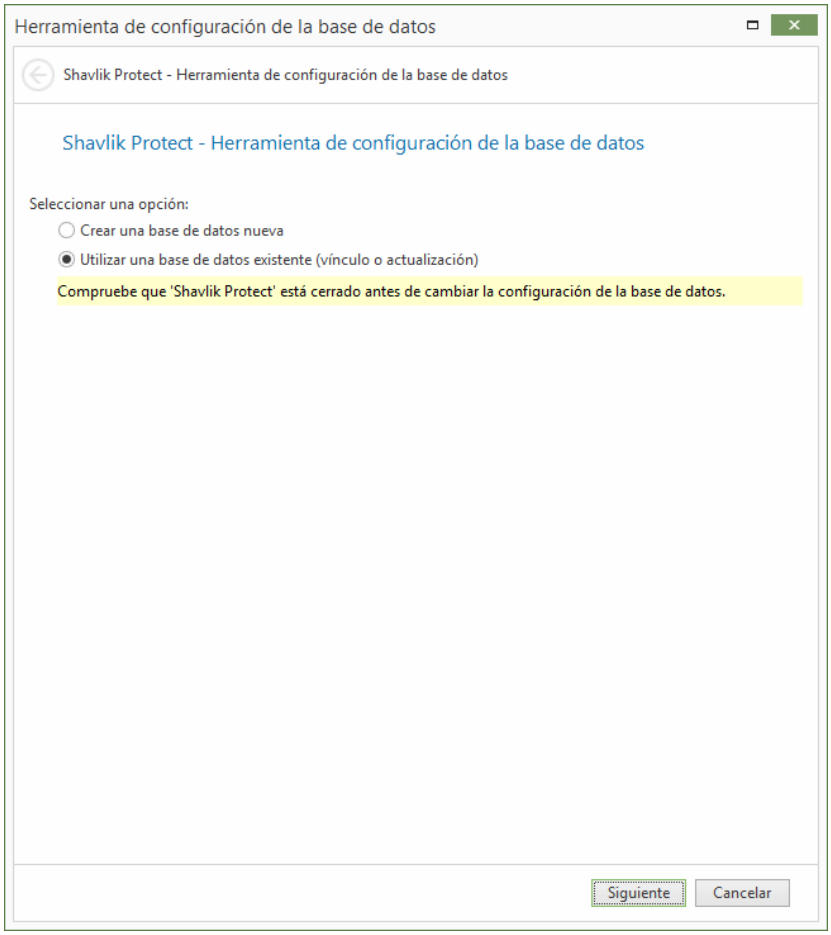
    Aparece el cuadro de diálogo **Programa de mejora del producto**. Lea la descripción e indique si está de acuerdo en participar en el programa. El programa permite a Shavlik recopilar información sobre el uso del producto que ayudará a mejorar futuras versiones.

11. Haga clic en **Siguiente**.

    Aparece el cuadro de diálogo **Preparado para realizar la instalación**.

12. Para comenzar la instalación, haga clic en **Instalar**.

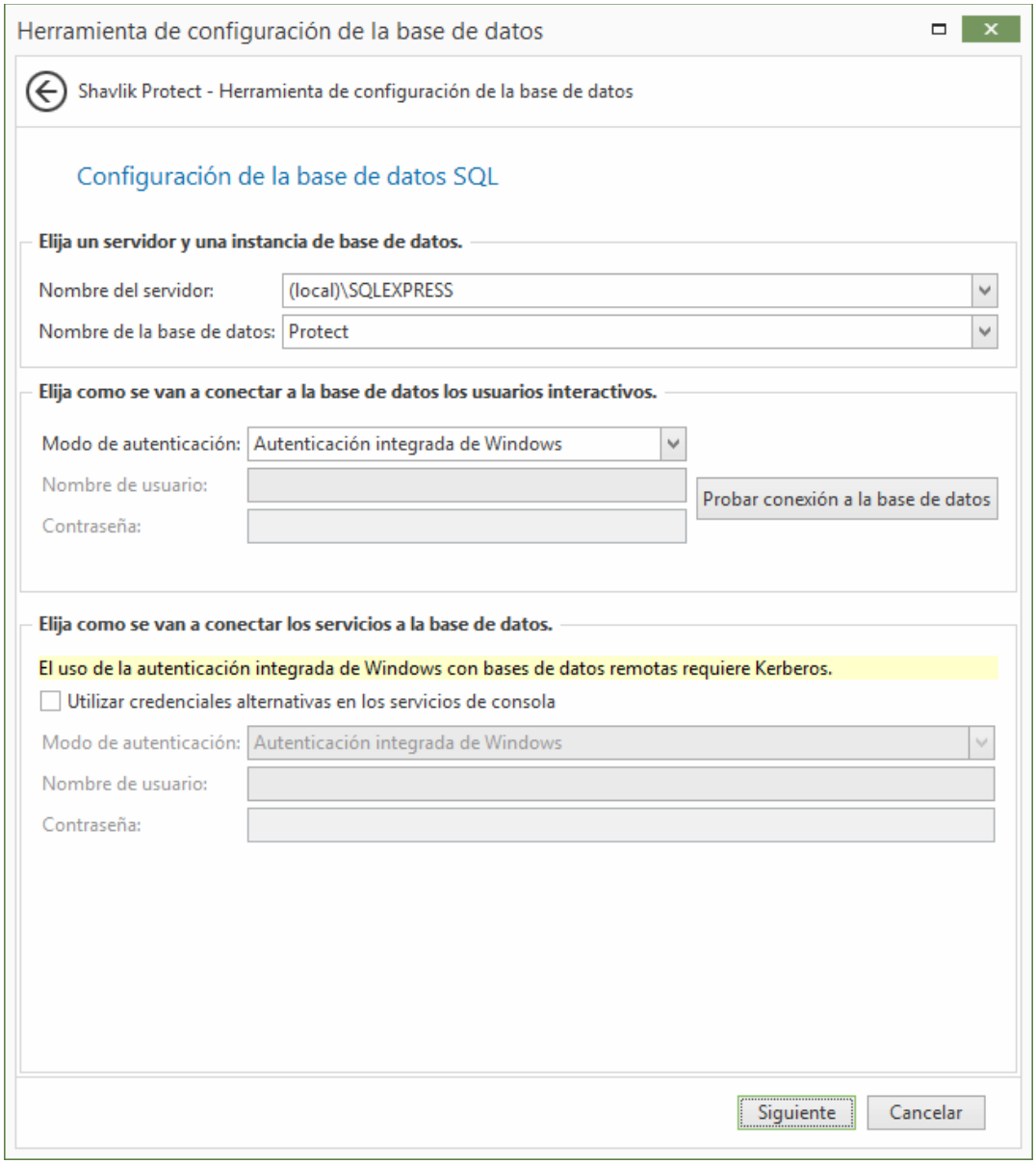
    Casi al final del proceso de instalación, aparece el cuadro de diálogo **Herramienta de configuración de la base de datos**.



Importante: En el siguiente paso, **no** seleccione **Crear una base de datos nueva**. Si lo hace, se creará una base de datos nueva y no se utilizarán los datos existentes.

13. Compruebe que ha seleccionado **Usar una base de datos existente** y a continuación, haga clic en **Siguiente**.

    Aparece un cuadro de diálogo similar a este:



14. Utilice los cuadros para definir cómo van a acceder los usuarios y los servicios a la base de datos SQL Server.

    Elija un servidor y una instancia de base de datos.

    - **Nombre del servidor:** se puede especificar un equipo, o un equipo y la instancia de SQL Server que se ejecuta en ese equipo.
    - **Nombre de la base de datos:** indique la base de datos que va a utilizar. El nombre predeterminado de la base de datos es **Protect**.

Elija cómo se van a conectar a la base de datos los usuarios interactivos.

Especifique las credenciales que va a utilizar el programa cuando un usuario realice una acción que requiera acceso a la base de datos.

- **Autenticación integrada de Windows:** es la opción recomendada y predeterminada. Shavlik Protect utilizará las credenciales del usuario que ha iniciado sesión para conectarse a la base de datos SQL Server. Los cuadros **Nombre de usuario** y **Contraseña** no estarán disponibles.
- **Usuario específico de Windows:** seleccione esta opción solo si la base de datos SQL Server está en un equipo remoto. Esta opción no tendrá ningún efecto si la base de datos están en el equipo local (consola). (Para obtener más información acerca de las credenciales del equipo local, consulte *Suministro de credenciales* en la **Guía de administración de Shavlik Protect**.) Todos los usuarios de Shavlik Protect utilizarán las credenciales suministradas cuando realicen acciones que requieran interactuar con la base de datos SQL Server remota.
- **Autenticación SQL:** seleccione esta opción para introducir la combinación de nombre y contraseña de usuario que se utilizará cuando se inicia sesión en el SQL Server especificado.

  Precaución: Si proporciona credenciales de autenticación SQL y no ha implementado el cifrado SSL para las conexiones SQL, las credenciales se transmitirán por la red en texto sin cifrar.
- **Probar conexión a la base de datos;** para comprobar que el programa puede utilizar las credenciales de usuario interactivo suministradas para conectarse a la base de datos, haga clic en este botón.

Elija cómo se van a conectar los servicios a la base de datos.

Especifique las credenciales que van a utilizar los servicios que se ejecutan en segundo plano cuando se conecten a la base de datos. Estas son las credenciales que utilizarán el importador de resultados, varias operaciones de agente y otros servicios para iniciar sesión en SQL Server y proporcionar el estado.

- **Utilizar credenciales alternativas en los servicios de consola:**
  - Si la base de datos SQL Server está instalada en el equipo local, lo normal es ignorar esta opción y no marcar esta casilla de verificación. En este caso, se utilizarán las mismas credenciales y método de autenticación que se especificó antes para los usuarios interactivos.
  - Marque esta casilla de verificación solo si la base de datos SQL Server está en un equipo remoto. Si la base de datos está en un equipo remoto, necesitará una cuenta que pueda autenticarse ante la base de datos del servidor remoto.
- **Método de autenticación:** solo está disponible si se habilita **Utilizar credenciales alternativas en los servicios de consola**.
  - **Autenticación integrada de Windows:** si selecciona esta opción, se utilizará la cuenta de equipo para conectar con el SQL Server remoto. El protocolo de autenticación de red Kerberos debe estar disponible para transmitir las credenciales de forma segura. Los cuadros Nombre de usuario y Contraseña no estarán disponibles.

Nota: Si selecciona **Autenticación integrada de Windows**, el programa de instalación intentará crear un inicio de sesión de SQL Server para la cuenta de equipo. Si el proceso de creación de la cuenta fracasa, consulte *Notas posteriores a la instalación de SQL Server* en la

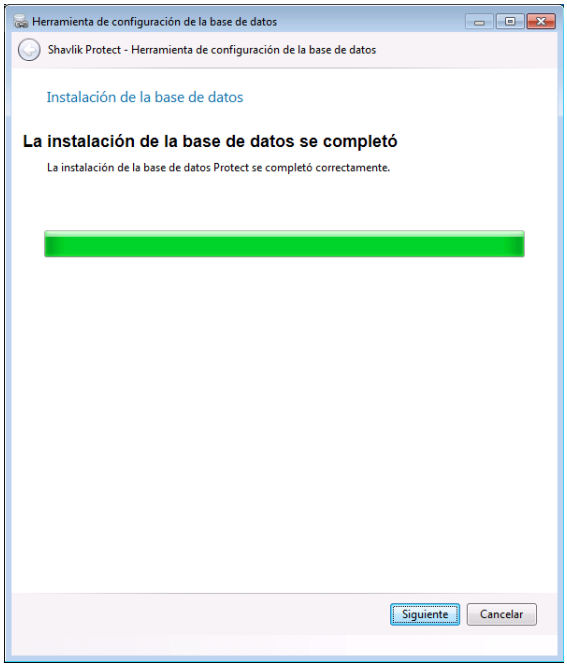
Guía de instalación de Shavlik Protect 9.2 para obtener instrucciones sobre cómo configurar manualmente un SQL Server remoto para que acepte credenciales de cuenta de equipo. Esto hay que hacerlo después de que termine el proceso de actualización de Shavlik Protect, pero antes de iniciar el programa.

- **Usuario específico de Windows:** seleccione esta opción para introducir una combinación específica de nombre y contraseña de usuario. Los servicios de Shavlik Protect que se ejecutan en segundo plano utilizarán estas credenciales para conectarse a la base de datos SQL Server. Esta es una buena opción alternativa si, por algún motivo, tiene dificultades para implementar la autenticación integrada de Windows.
- **Autenticación SQL:** seleccione esta opción para proporcionar la combinación de nombre y contraseña específicos que se utilizarán para iniciar sesión en SQL Server.

15. Después de proporcionar toda la información requerida, haga clic en **Siguiente**.

Nota: Si el programa de instalación detecta un problema con cualquiera de las credenciales especificadas, aparecerá un mensaje de error. Esto suele indicar que la cuenta de usuario especificada no existe. Corríjala e inténtelo de nuevo.

La consola está vinculada con la base de datos. Una vez terminado el proceso de vinculación, aparece el cuadro de diálogo siguiente:.



16. Haga clic en **Siguiente**.
17. En el cuadro de diálogo **Instalación completada**, haga clic en **Finalizar**.
18. En el cuadro de diálogo **Asistente para la instalación de Shavlik Protect completada**, marque la casilla de verificación **Iniciar Shavlik Protect** y a continuación, haga clic en **Finalizar**.

TAREAS DE ACTUALIZACIÓN EN LA CONSOLA

Para completar la actualización, es necesario realizar las tareas siguientes en la consola de Shavlik Protect.

Asignar credenciales del programador

Para ejecutar las tareas de la consola del programador, es necesaria una credencial de programador que coincida con la cuenta del usuario actual. Si hay tareas programadas en la consola y no se ha ajustado la credencial del programador, recibirá un aviso durante el inicio para que ajuste la credencial. Esta comprobación se produce cada vez que se inicia Shavlik Protect para garantizar que las tareas programadas sigan ejecutándose.

Revise las tareas programadas

Las tareas programadas ahora se controlan y se administran desde dos áreas diferentes. Deberá comprobar los dos administradores de tareas programadas para verificar que las tareas existentes tienen el puerto correcto.

- El **Administrador de tareas de consola programadas** proporciona una ubicación para ver las tareas que estén programadas actualmente en la consola, como los análisis de parches, de activos; los despliegues de parches al equipo de la consola, la ejecución de secuencias de comandos y los informes programados.
- El **Administrador de tareas remotas programadas** proporciona una ubicación desde la que supervisar las tareas de energía y las tareas de despliegue de parches programadas actualmente en el equipo de destino remoto.

Actualice la licencia (solo consolas desconectadas)

Si la consola está desconectada (no tiene conexión a Internet), para ver y utilizar las funciones nuevas de Shavlik Protect 9.2, la licencia debe actualizarse manualmente. Para obtener más información acerca de la activación de consolas desconectadas, en el sistema Ayuda, vea **Instalación y configuración** > **Tareas iniciales** > **Activación del programa**.

Si la consola está conectada, la licencia se actualiza automáticamente durante el proceso de actualización.

Revise las Plantillas de análisis de parches y los Grupos de parches

Hay tres cuestiones a tener en cuenta en estas áreas.

- **Plantilla de análisis de parches:** La pestaña **Filtrar** del diálogo **Plantilla de análisis de parches** se ha actualizado para permitir una mayor precisión durante el análisis. Aunque el proceso de actualización convertirá automáticamente las plantillas de análisis de parches existentes al nuevo estilo, deberá comprobar las plantillas para verificar los cambios.
- **Grupos de parches:** Los grupos de parches ya no se definen mediante un diálogo diferente, en lugar de eso, ahora se crean y se administran desde el interior de la Vista Parche. Aunque el proceso de actualización convertirá automáticamente los grupos de parches existentes a la nueva convención, deberá comprobar los grupos para verificar los cambios. Los grupos de parches pueden ser más pequeños después de la actualización, ya que Shavlik ha dejado de dar soporte de muchos parches antiguos.

- **Grupos de parches modificados y generados automáticamente:** Para mantener el comportamiento de las plantillas de análisis de parches, se pueden modificar uno o más grupos de parches existentes durante el proceso de actualización y generar automáticamente uno o más grupos de parches nuevos.
    - **Grupos de parches modificados:** Si hace referencia a un grupo de parches de la sección **Configuración del filtro de parches** de la plantilla de análisis de parches versiones 9.0 y 9.1 y se habilita **Analizar seleccionados**, los parches que no cumplan con los criterios definidos por los filtros de la plantilla de análisis se eliminarán del grupo. Este es el motivo: En Protect 9.0 y 9.1, los filtros de la plantilla de análisis pueden enmascarar el hecho de que el grupo de parches pueden contener tipos de parches que no pretendía que llevasen a cabo un análisis o un despliegue. En Protect 9.2, cuando se utiliza un grupo de parches como línea base, los filtros de la plantilla de análisis no se aplicarán y es posible que se revelen las imprecisiones de los grupos de parches. Si el proceso de actualización detecta esta situación, automáticamente modificará el grupo de parches para mantener la interacción deseada entre la plantilla de análisis y el grupo de parches.

      Ejemplo:

      Imagine que su grupo de parches 9.1 contiene una mezcla de parches de seguridad, no seguridad y distribución de software. En la plantilla de análisis a la que haga referencia este grupo de parches, la sección **Configuración del filtro de parches** se ajusta como **Analizar seleccionados** y la sección **Propiedades del parche** se ajusta para que detecte sólo los parches de seguridad. En esta configuración, se seguirá el filtro **Propiedades del parche** y sólo se detectarán los parches de seguridad, a pesar del hecho de que el grupo de parches contiene parches de no seguridad y de distribución de software.

      Después de actualizar a 9.2, la plantilla de análisis definirá el grupo de parches como un filtro de línea base y el resto de filtros de la plantilla de análisis se ignorarán. Si el grupo de parches no se modifica, los parches de no seguridad y de distribución de software se detectarán, y se desplegarán si habilita la casilla **Desplegar los parches automáticamente después del análisis** cuando realice un análisis. El proceso de actualización reconocerá esta discrepancia y eliminará los parches de no seguridad y de distribución de software del grupo de parches.

      Nota: Cuando avance, tenga cuidado y administre correctamente los grupos de parches evitando agregar los parches innecesarios o no deseados o tipos de parches.

- **Grupos de parches generados automáticamente:** Si se cumplen las condiciones siguientes, con el proceso de actualización se generará automáticamente una copia de un grupo de parches existente:
  - Si el grupo de parches tiene referencia en una sección de **Configuración del filtro de parches** de una plantilla de análisis de parches y **Analizar seleccionado** está habilitado.
  - Si el grupo de parches tiene referencia en una política de agentes o en una segunda plantilla de análisis que contenga diferentes definiciones de filtros.
  - Si se debe modificar el grupo de parches mediante un proceso de actualización para mantener la compatibilidad (ver arriba).

  En esta situación, se generará una copia del grupo de parches y luego se modificará tal y como se describe más arriba. El nombre del nuevo grupo de parches será ***<nombre del grupo de parches> -generados para <nombre de la plantilla de análisis>**. Las plantillas de análisis que hacen referencia al grupo de parches se actualizarán para que utilicen el nuevo nombre de grupo de parches. El grupo de parches original se mantiene para que haga referencia a las políticas de agente u para que se mantengan otras plantillas de análisis.

  Deberá revisar los cambios y, si así lo desea, cambiar el nombre del grupo de parches generado automáticamente a uno más fácil de recordar.

Asigne de alias a la consola

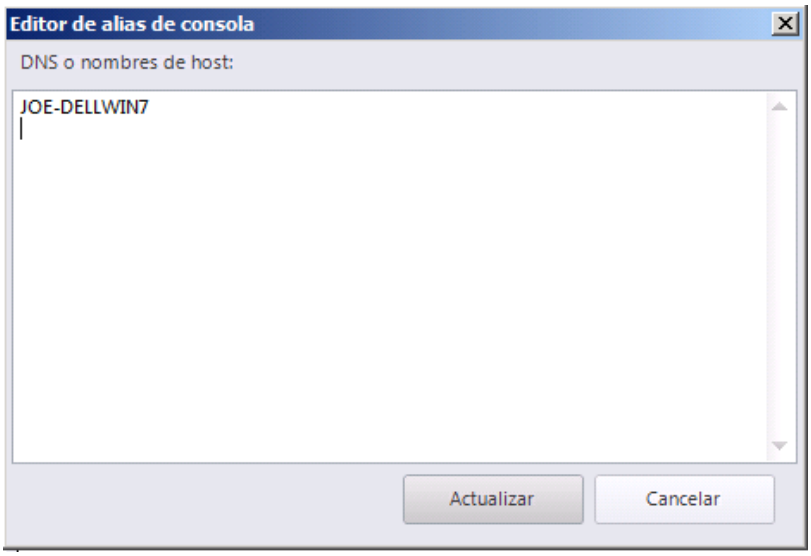
Esta tarea es necesaria si se dan una o más de las condiciones siguientes:

- Ha asignado el equipo de la consola a un dominio nuevo
- Ha dado un nuevo nombre común o dirección IP a la consola
- Ha instalado manualmente agentes y estos utilizan una dirección IP para comunicarse con la consola

En estas condiciones, debe utilizar la herramienta **Editor de alias de la consola** para identificar los nombres antiguos o las direcciones de la consola como alias de confianza. De lo contrario, cuando un agente se conecta a la consola de Shavlik Protect o un equipo sin agente intenta enviar mensajes de estado del despliegue de parches a la consola, no podrán verificar si el equipo con el que contactaron es un equipo de confianza.

1. Seleccione **Herramientas > Editor de alias de consola**.

   Aparece el cuadro de diálogo **Editor de alias de consola**. Contiene los nombres y las direcciones IP utilizadas actualmente para identificar el equipo de la consola. Por ejemplo:

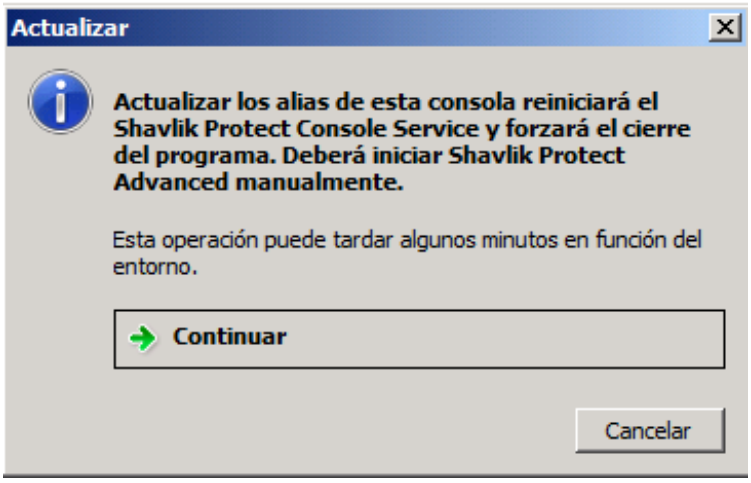


2. Escriba los nombres o direcciones IP que se van a utilizar como alias del equipo de consola.

   Las direcciones IP pueden especificarse utilizando el formato IPv4 o IPv6.

3. Haga clic en **Actualizar**.

   Aparece el siguiente cuadro de diálogo.



Para actualizar los alias de la consola, se debe reiniciar el servicio de la consola. Shavlik Protect debe cerrarse y reiniciarse manualmente.

IMPORTANTE Los agentes no reconocerán los alias nuevos hasta que no se pongan en contacto con la consola reiniciada. El contacto debe ser iniciado por un agente. Puede hacerse manualmente mediante el programa de cliente del agente, o mediante un contacto programado. Un comando de contacto enviado desde la consola a un agente no actualiza el certificado de la consola.

Sincronice los servidores de distribución

Debe actualizar los servidores de distribución con los parches y/o motores de análisis más recientes y los archivos de definición XML de la consola. Esto es especialmente importante si los agentes utilizan servidores de distribución para descargar estos archivos. Los servidores de distribución deben estar sincronizados con los archivos de la consola actualizados **antes** de que los agentes se conecten.

Para sincronizar los servidores de distribución:

1. Seleccione **Ayuda > Actualizar archivos** para asegurarse de que la consola contenga todos los archivos más recientes.
2. Seleccione **Herramientas > Operaciones > Servidores de distribución**.
3. En el cuadro **Agregar sincronización programada** del panel superior, seleccione el componente que desea sincronizar.
4. En el panel superior, seleccione qué servidor de distribución se va sincronizar con la consola.
5. Haga clic en **Agregar sincronización programada**.
6. Indique cuándo desea que se produzca la sincronización y haga clic en **Guardar**.
7. En el panel **Sincronización automática programada**, seleccione la entrada de sincronización programada.
8. Haga clic en **Ejecutar ahora**.

No se preocupe si los agentes se conectan antes de que haya terminado de sincronizar los servidores de distribución. Los agentes se actualizarán la próxima vez que se ejecute una tarea programada o que el agente actualice sus binarios.

Contemple la posibilidad de habilitar la función de Parche predictivo

Esta nueva función permite a Shavlik Protect descargar automáticamente parches que se pueden desplegar en un futuro próximo. Si utiliza servidores de distribución, puede sincronizar Parche predictivo con los servidores de distribución para que reciban copias de los parches descargados La opción de Parche predictivo se activa en la pestaña **Herramientas > Operaciones > Descargas** y se sincroniza con los servidores de distribución habilitando la opción **Sincronizar con Parche predictivo** del diálogo **Servidor de distribución.** Para toda la información, consulte la Ayuda del sistema.

Vuelva a establecer la seguridad entre las consolas de datos de consolidación

Si utiliza varias consolas y tiene activada una configuración de consolidación de datos, deberá volver a establecer la asociación de seguridad entre la consola central y cada consola remota.

IMPORTANTE Cuando haya empezado el proceso de actualización, no se producirá actividad de consolidación de datos hasta que la consola central y la remota se hayan actualizado y se haya vuelto a establecer la asociación de seguridad entre las dos consolas. Por este motivo, es recomendable que actualice las consolas juntas y a una hora a la que espere poca actividad de consolidación de datos.

En la consola central

1. Actualice la consola central.
2. Seleccione **Herramientas > Operaciones > Consolidación de datos** y verifique que la casilla **Aceptar e importar resultados desde un emisor de consolidación** esté marcada.

En cada consola remota

1. Actualice todas las consolas remotas.
2. Seleccione **Herramientas > Consolidación de datos**.
3. Especifique la dirección IP/nombre del host y el número de puerto que utilizará la consola de consolidación.
4. Haga clic en **Registrar**.

Para obtener más información acerca de la consolidación de datos, en Ayuda del sistema, consulte **Administración de varias consolas > Configuración de consolidación de datos.**

Analice las máquinas virtuales

Si ha definido equipos virtuales en un grupo de equipos en la pestaña **Máquinas virtuales alojadas** o en la pestaña **Máquinas virtuales de estación de trabajo**, después de llevar a cabo la actualización, deberá iniciar un análisis de estos equipos desde la página de inicio o desde el grupo de equipos. Es necesario hacer esto para volver a establecer las identidades de los equipos con Protect. Si no lleva a cabo el análisis, es posible que no se muestren los campos **Servidor virtual** y **Ruta** en la vista Equipo y el despliegue en estos equipos podría fallar.

Compruebe la configuración de usuario personalizada

La siguiente configuración del usuario personalizado no se guarda durante la actualización.

- Herramientas > Opciones > Pestaña mostrar pestaña:
  - Elementos recientes (días)
  - Archivar elementos
  - Mostrar solo los elementos creados por mí
  - Mostrar la fuente de noticias principal
  - Mostrar elementos informativos en los resultados de los análisis de parches
  - Mostrar service packs en Vista > Parches
- Herramientas > Opciones > Pestaña de notificaciones y advertencias:
  - Avisar antes de programar despliegues
  - Cerrar los archivos de la actualización al terminar
  - Avisar si la sincronización con Protect Cloud no está habilitada en esta consola
  - Avisar antes de abrir 7 boletines o más
- Herramientas > Opciones > Pestaña inicio de sesión:
  - Análisis de parches de diagnóstico
- Supervisor de despliegues:
  - Velocidad de la actualización
  - Días que se van a mostrar
  - Mostrar errores
  - Mostrar en progreso
  - Mostrar los completados correctamente
- Cuadro de diálogo Informes
  - Ordenar por id. de IAVA
- Pestaña boletín del hipervisor ESXi:
  - Mostrar solo los más recientes
- Historial de eventos
  - Limitar los resultados a los (días) anteriores:
- Vista Resultados de ITScripts
  - Resultados desde

Protect 9.2 utiliza un certificado de raíz SHA-2

Shavlik ha introducido el uso de certificados SHA-2 de raíz y de consola en Protect 9.2. Esto se debe a dos motivos principales: los certificados SHA-2 de 2048-bit son más seguros que su antecesor, el SHA-1 de 1024-bit, y los certificados de raíz SHA-1 han quedado obsoletos y Windows dejará de aceptarlos a partir del 1 de enero de 2017.

Una vez completado el proceso de actualización, Shavlik Protect 9.2 empezará su propio proceso, en segundo plano, para emitir un nuevo certificado de raíz SHA-2 y un nuevo certificado de consola SHA-2. Si no utiliza agentes, este proceso será invisible y se puede ignorar. Si utiliza agentes, parte del proceso incluye esperar a que los agentes se conecten para que puedan recibir el nuevo certificado de raíz pendiente. Este proceso puede tardar días o semanas, según una serie de factores, pero se ejecutará en segundo plano. Lo único que debe hacer es vigilar el registro Historial de eventos para ver si se produce algún problema que requiera su atención.

CAMBIOS Y MEJORAS SIGNIFICATIVOS EN SHAVLIK PROTECT 9.2

En Ayuda del sistema encontrará toda la información acerca de los temas siguientes:

http://help.shavlik.com/Protect/onlinehelp/92/ENU/PRT.htm

Despliegues de parches	Se ha vuelto a escribir todo el motor de empaquetado y despliegue de parches en equipos. Se han mejorado el rendimiento y la fiabilidad.
Contenido de parches	Los datos de evaluación y despliegue de parches que Shavlik Protect consume se han vuelto a empaquetar y se han mejorado de muchas maneras.
Filtrado de la plantilla de análisis de parches	Se han añadido más metadatos al contenido de los parches. Además, la pestaña **Filtrar** del diálogo **Plantilla de análisis de parches** se ha actualizado para permitir una mayor precisión durante el análisis.
Vista Parches / Grupo de parches	La vista Parches se ha rediseñado y actualizado completamente. Aprovecha el nuevo formato de contenido, lo que le permite ver la información de parches de manera más concreta. Además, los grupos de parches ahora se crean y se administran desde la vista Parches. Esto le permite investigar parches y crear grupos de parches de manera más unificada.
Tareas programadas	Las tareas programadas de la consola ahora utilizan el Programador de tareas de Microsoft. Un nuevo diálogo, disponible desde el menú **Administrar > Tareas de consola programadas**, le permite ver y administrar estas tareas.
Informes	Hay disponible un nuevo informe de **Fin de la vida por Producto.** Además, un nuevo diálogo de **Programar informe**, disponible en el menú **Herramientas > Programar informe**, le permite generar un informe automáticamente a una hora en el futuro. El informe se puede generar automáticamente una vez o de manera regular.
Parche predictivo	Esta nueva opción permite a Shavlik Protect descargar automáticamente parches que se pueden desplegar en un futuro próximo. Descargar los parches antes del despliegue ayudará a mejorar la velocidad del proceso de despliegue.
Programación de Patch Tuesday + X (días)	Cuando se programan análisis de consola, se puede retrasar un análisis recurrente un número de días para que coincida con un acontecimiento periódico. Por ejemplo, puede ejecutar un análisis de parches mensuales el día después de Patch Tuesday, mediante la opción **Agregar retraso (días).**

Notificación de final del ciclo de vida

Cuando la versión de Shavlik Protect que está utilizando se esté acercando a la fecha del final de su ciclo de vida (EOL), cuando inicie Shavlik Protect aparecerá un mensaje.

Integración con Protect Cloud

El análisis de parches y los resultados del despliegue se pueden enviar regularmente a Protect Cloud. Si es usuario de Shavlik Empower, Empower recuperará periódicamente los datos del parche de Empower desde Protect Cloud y los datos se podrán ver con la interfaz del usuario de Shavlik Empower basada en el explorador.

Cambios en la interfaz del usuario

Los siguientes elementos de la interfaz del usuario se han modificado:

- La vista Parches se ha rediseñado completamente.
- Los grupos de parches ahora se crean y se administran desde la vista Parches.
- En vista Equipos:
    - El panel superior contiene tres columnas nuevas: Servidor virtual, Nombre de VM y Parche
    - La pestaña **Activos virtuales** se ha eliminado del panel intermedio
    - En el panel inferior, las pestañas **Equipos ausentes** y **Equipos instalados** se han combinado en una nueva pestaña denominada **Equipos afectados.**
- En la plantilla de despliegue de parches:
    - Se ha eliminado la compatibilidad con los Puntos de instalación de Office y con Medios originales.
    - Se han eliminado las opciones **Hacer copia de seguridad de archivos para la desinstalación** y **Modo silencioso**, ahora siempre están activas.
    - Se ha rediseñado la pestaña **Servidores de distribución** para ayudar a identificar el orden en que se utilizarán las fuentes de descarga.
- En la plantilla de análisis de parches:
    - La pestaña Filtrado se ha rediseñado completamente
    - Se ha eliminado la criticidad de usuarios
    - La pestaña Distribución de software sólo muestra los productos que no se han sustituido.
- En una política de agentes, ahora todas las tareas pueden crearse sin un programa periódico. Esto le permite definir las tareas que se ejecutarán sólo a través de la interfaz del usuario del agente o mediante la iniciación de tareas remota desde la consola.
- En un grupo de equipos, se han combinado las opciones **Probar si existe** y **Probar credenciales** y se implementan llevando a cabo un análisis del estado de energía.

- Los resúmenes de activos virtuales ya no están disponibles en la vista Equipo. Ahora, toda la información de activos virtuales está disponible mediante la función Inventario virtual.
- Se han eliminado los informes Detalles del hardware de máquinas virtuales, Uso de memoria de máquinas virtuales y Uso de discos de máquinas virtuales
- En la vista Análisis, el panel secundario Resumen de análisis ya no se despliega
- Las tareas programadas están separadas en dos diálogos diferentes: **Administrar > Tareas remotas programadas** y **Administrar > Tareas de consola programadas**
- En **Herramientas > Opciones**:
    - **Mostrar:** Contiene una nueva casilla denominada **Mostrar service packs en Vista > Parches**
    - **Notificaciones y advertencias:** Contiene una nueva casilla denominada **Avisar antes de abrir 7 boletines o más** y se ha eliminado la casilla **Advertir antes de programar operaciones cuando las credenciales predeterminadas no coincidan con el usuario actual**
    - **Idiomas del parche:** Esta pestaña se ha eliminado. Ahora el programa detectará automáticamente los idiomas del sistema operativo que se utilicen en los equipos administrados y descargará sólo las versiones necesarias del idiomas del archivo de parche.
    - **Análisis:** Contiene una nueva casilla denominada **Forzar siempre las exclusiones de grupos de equipos**
    - **Despliegue:** Se ha eliminado la opción **Dirección del Supervisor de despliegues.** Ahora la dirección se define mediante el **Editor de alias de la consola.**
    - **Registro:** Contiene una nueva casilla denominada **Análisis de parches de diagnóstico**