

SavClean

Aplicación para desinstalar de forma efectiva el producto antivirus Sav32 12.1.

Este programa finaliza los procesos relacionados con Sav32 12.1 si están en ejecución, detiene los servicios, elimina las claves y valores del registro de Windows y borra permanentemente los ficheros y carpetas relacionadas con el antivirus.

Forma de uso:

Para desinstalar el antivirus Sav32 12.1, **SavClean** puede ser ejecutado manualmente presionando doble click sobre él, a través de un script de inicio de sesión asociado al perfil de una o varias cuentas de usuarios en el Directorio Activo (AD) o a través de un script de inicio de sesión asociado a un Objeto de Política de Grupo (GPO).

Descripción:

1. Ejecución manual.
2. Uso de un script de inicio de sesión asociado al perfil de una cuenta de usuario.
3. Uso de un script de inicio de sesión asociado a un Objeto de Política de Grupo.

Ejecución manual:

Al ejecutar manualmente la aplicación se observa la ventana que se muestra a continuación. Ver figura 1.



Figura 1. Ventana principal de SavClean.

Al presionar el botón `Comenzar Limpieza` se inicia el proceso de desinstalación mostrando con color azul el texto correspondiente a la acción en curso (Ver figura 2). Una vez finalizada se ubica a su derecha una marca ✓ que puede ser roja o verde, en dependencia del estado en que haya concluido dicha operación. Consultar el [anexo 1](#) para más detalles.



Figura 2. Ventana que muestra la ejecución de las tareas y el estado en que concluyen las mismas.

Seguidamente el botón se inhabilita y cambia el nombre por `Mostrar Fichero Log`, (Ver figura 2) permitiéndole al usuario cuando se habilita observar en una nueva ventana las modificaciones realizadas en el sistema al terminar la desinstalación. Ver figura 3.

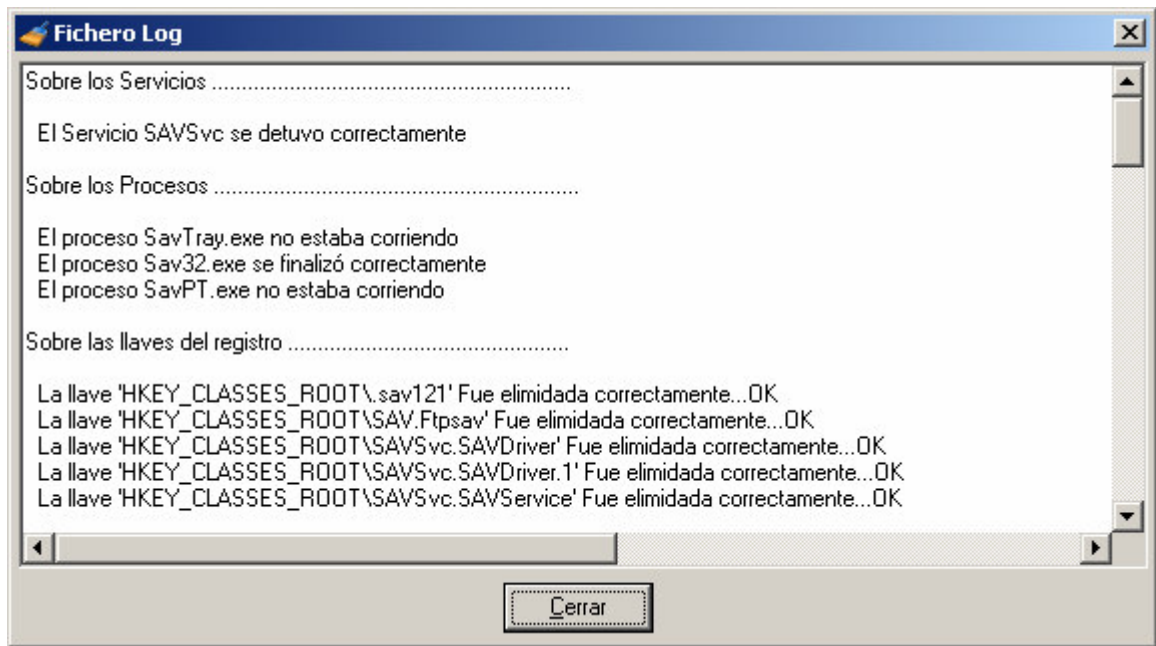


Figura 3. Ventana que muestra el fichero log.

En dependencia de los cambios realizados, al cerrar la aplicación, se le pedirá confirmación al usuario para reiniciar el sistema. Ver figura 4.

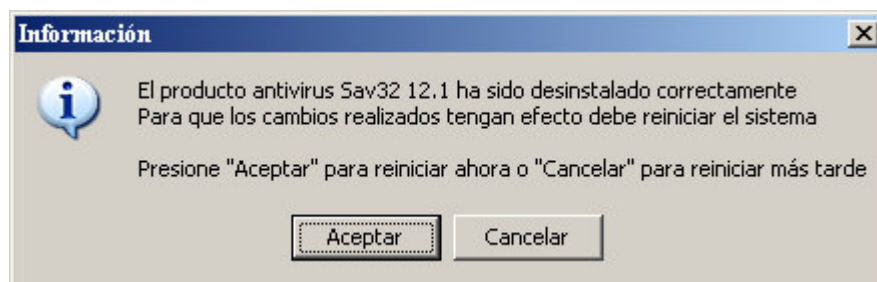


Figura 4. Confirmación de reinicio del sistema.

Uso de un script de inicio de sesión asociado al perfil de una cuenta de usuario.

Este método se basa en un mecanismo propio del Directorio Activo, el cual garantiza la instalación o desinstalación de software en las PCs de los clientes de manera remota.

Se debe utilizar un script asociado al perfil de una o varias cuentas de usuarios para ejecutar la instalación remota con el inicio de sesión. El procedimiento a seguir es el siguiente:

2.a. Crear en el subdirectorio del dominio asociado a los scripts, usualmente en una ubicación al estilo de **\\servidordominio\sysvol\nombredominio\scripts**, un fichero de extensión **.bat** (savclean.bat, por ejemplo) con un contenido similar al siguiente:

```
@echo off
REM Copyright (C) 2007 Segurmatica
REM
REM echo Desinstalación del Antivirus Sav32 12.1
start \\servidor\savclean\savclean.exe [parámetros_opcionales]
```

Los campos de interés para este punto son los siguientes:

- **servidordominio:** Nombre (o dirección IP) del servidor controlador de dominio.
- **nombredominio:** Nombre del dominio. Ejemplo: segurmatica.cu
- **servidor: Nombre** (o dirección IP) que tiene el recurso compartido "savclean" con el fichero ejecutable en su interior.
- **[parámetros_opcionales]:** Se pueden establecer un conjunto de parámetros para controlar el transcurso de la desinstalación de la siguiente manera:

/reboot_auto: Reinicia la maquina automáticamente al finalizar la desinstalación.

/reboot_confirm: Le pide confirmación de reinicio al usuario, pudiendo este posponerlo para otro momento.

/createlog: Crea un fichero log llamado savclean.log con la descripción de todos los cambios realizados en el sistema en la ubicación %systemroot%\Temp\. Por ejemplo: C:\Windows\Tem\savclean.log

Sin especificar opciones: El desinstalador se ejecuta de manera similar al procedimiento descrito en la [ejecución manual](#).

Consulte el apartado [Notas Importantes](#) para más detalles.

2.b. Asociar el script anterior al inicio de sesión de una cuenta de usuario: especificar su nombre (savclean.bat, por ejemplo) en el cuadro de texto relativo a *Script de inicio de sesión* en la pestaña *Perfil* de las *Propiedades* de una cuenta de usuario en el Directorio Activo.

Esta operación se puede aplicar de una vez a todos los usuarios de una Unidad Organizativa del Directorio Activo si en el Controlador de Dominio se ejecuta un script (con nombre savclean.vbs, por ejemplo). Consultar el [anexo 2](#) para mas detalles.

2.c. Reiniciar la sesión; con ello comienza el proceso de desinstalación.

Uso de un script de inicio de sesión asociado a un Objeto de Política de Grupo.

Este método también se basa en un mecanismo propio del Directorio Activo para la instalación y desinstalación remota. El método es válido solo para los sistemas del tipo Microsoft Windows NT (Windows NT y Windows 2000 o superior, en todas sus ediciones) y es el recomendable si la red está compuesta únicamente por dichos sistemas pues incluye las potencialidades inherentes a las políticas de grupo del Directorio Activo.

Se debe utilizar un script asociado a la Configuración de Usuario de un Objeto de Política de Grupo del Directorio Activo para ejecutar la desinstalación con el inicio de sesión. El procedimiento a seguir es el siguiente:

3.a. Ejecutar el punto 2.a del procedimiento anterior.

3.b. Asociar el script anterior (savclean.bat) al `Script de Inicio de Sesión de la Configuración de Usuario` del Objeto Política de Grupo correspondiente a la Unidad Organizativa del Directorio Activo a la cual pertenecen las cuentas de usuario que ejecutarán la desinstalación con el inicio de sesión.

3.c. Ejecutar el punto 2.c del procedimiento anterior.


Notas Importantes

1. El programa fue probado siendo exitoso el resultado en Windows 2000, Windows XP y Windows 2003 Server. En Windows 9x o Me no funcionará la aplicación por ejecutar acciones no compatibles con dichos sistemas.
2. El usuario con el que se realiza la desinstalación debe tener suficientes privilegios como para llevar a cabo las tareas que se ejecutan en el transcurso de la misma. Ejemplo: Ser miembro del grupo local Administradores.
3. Si se ejecuta la desinstalación en varias estaciones de trabajo de forma centralizada (Utilizando el directorio Activo) se deben tener en cuenta los siguientes aspectos al pasarle los parámetros a la aplicación en la configuración del script:
 - Se pueden agrupar varios parámetros sin tener en cuenta el orden en que se escriben.
 - Cada parámetro debe estar precedido por un espacio, de lo contrario será ignorado. Ejemplo:

```
start \\servidor\savclean\savclean.exe /reboot_confirm /createlog
```
 - Si los parámetros /reboot_auto y /reboot_confirm están presentes, reboot_auto tiene prioridad y /reboot_confirm será ignorado.
 - Si no se especifican parámetros o si ninguno de los parámetros pasados coincide con los mencionados anteriormente, serán ignorados y la aplicación se ejecutara de forma similar al procedimiento descrito en la [ejecución manual](#).
4. Todas las máquinas donde se desinstale el producto antivirus de forma centralizada tienen que ser miembros del dominio.

Anexo 1. Significado del color de la marca a la derecha de las acciones a ejecutar por el desinstalador del antivirus al finalizar.

 Significa que todas las tareas realizadas tuvieron éxito.

 Significa que alguna tarea realizada no tuvo éxito aunque no siempre se relaciona con un error.
Ejemplo:

Deteniendo Procesos:

- El usuario actual no cuenta con los suficientes permisos para finalizar el proceso.
- No se pudo cargar la biblioteca PSAPI.DLL para finalizar el proceso.
- El proceso relacionado no se pudo finalizar por razones desconocidas.
- El nombre del proceso no es válido.
- No se pudo obtener la dirección del proceso desde PSAPI.DLL.
- No se pudo obtener la lista de procesos activos.
- No se pudo cargar la biblioteca KERNEL32.DLL para finalizar el proceso.
- No se pudo obtener la dirección del proceso desde KERNEL32.DLL.
- CreateToolhelp32Snapshot falló para el proceso relacionado.
- Error desconocido al tratar el proceso.

Deteniendo / Eliminando Servicios:

- El Servicio relacionado ya estaba detenido.
- El Servicio relacionado en este momento se está iniciando.
- El Servicio relacionado en este momento se está deteniendo.
- El estado de Servicio continúa pendiente.
- El Servicio relacionado se está poniendo en pausa.
- El Servicio relacionado está en pausa.
- El Servicio relacionado no existe en el sistema.

Limpiando el Registro:

- Error abriendo la llave. La llave del registro no fue encontrada.
- Algún valor del registro no fue encontrado.

Eliminando Ficheros:

- El directorio relacionado no fue encontrado.
- El directorio no estaba vacío.
- El usuario actual no cuenta con los suficientes permisos para eliminar los ficheros.

Toda la información relacionada al respecto puede ser consultada en el fichero log que genera la aplicación.

Anexo 2. Asociar el script anterior (savclean.bat) al inicio de sesión de todas las cuentas de usuarios pertenecientes a una Unidad Organizativa en el controlador de dominio.

```
'Script para asignar un único script de inicio de sesión
'a todos los usuarios de una Unidad Organizativa (OU):
'Definir LDAP, todo en una sola línea:
Set OU = GetObject("LDAP://servidor.segurmatica.cu/OU=prueba,DC=segurmatica,DC=cu")
'Para todos los usuarios de la OU:
For Each oUser In OU
If oUser.Class = "user" Then
'nombre del script de inicio de sesión:
oUser.Put "scriptpath", "savclean.bat"
'Aplicar configuración:
oUser.SetInfo
End If
Next
Wscript.echo "OU actualizada"
Wscript.Quit
```

Los campos de interés son los siguientes:

- `servidor.segurmatica.cu`: Nombre completo del servidor que actúa como Controlador de Dominio según el formato FQDN.
- `prueba`: Nombre de la Unidad Organizativa (OU) a la que pertenecen las cuentas de usuarios que ejecutarán el script de inicio de sesión único.
- `segurmatica` y `cu`: Todos los campos del dominio, según el DNS, que usa el Directorio Activo.

A cerca de...

Programa para desinstalar de forma efectiva el producto antivirus Sav32 12.1.

Copyright © 2007. Yusleivi Mompeller Aguiar

Especialista en seguridad informática.

Grupo Soporte Técnico. Segurmatica

Email: yusleivi@segurmatica.cu