

El servicio de conector de FireAMP no se puede detener debido a la protección del conector

Contenido

[Introducción](#)

[Configuración de la protección del conector](#)

[Controlador de autoprotección](#)

[Detención del servicio de conector de FireAMP](#)

[Razones para detener](#)

[Detener servicio mediante propiedades del conector](#)

[Detener servicio mediante CLI](#)

[Solución](#)

[Detenga el servicio mediante la línea de comandos](#)

[Detener servicio mediante la interfaz de usuario](#)

Introducción

El conector FireAMP tiene una función denominada **Protección de conectores**. Esta opción permite proteger el servicio de conector de FireAMP mediante contraseña y evitar que se detenga o desinstale. Sin embargo, puede afectar al proceso de resolución de problemas debido al hecho de que detener el servicio del conector de FireAMP o desinstalarlo puede llegar a reproducirse como un paso de solución de problemas. Este documento describe cómo desinstalar FireAMP cuando está protegido mediante contraseña.

Configuración de la protección del conector

Para habilitar la opción **Connector Protection**, edite su política, vaya a la pestaña **General** y expanda **Administrative Features**.

Administrative Features



Send User Name in Events	<input type="checkbox"/>	
Send Filename and Path Info	<input checked="" type="checkbox"/>	
Heartbeat Interval	15 minutes	
Confirm Cloud Recall™	<input type="checkbox"/>	
Connector Log Level	Default	
Tray Log Level	Default	
Connector Protection	<input checked="" type="checkbox"/>	
Connector Protection Password	

Controlador de autoprotección

La función de protección de conectores utiliza un controlador de autoprotección para proteger los directorios de FireAMP. Un controlador autoprotegido realiza las siguientes tareas:

1. Evite que se eliminen y modifiquen las claves del Registro que utiliza FireAMP.
2. Evite que las aplicaciones escriban o eliminen archivos en el directorio de instalación. El directorio de instalación predeterminado es:

```
"%PROGRAMFILES%\Sourcefire\FireAMP"
```

3. Evite descargar o sobrescribir los controladores de FireAMP.
4. Evite que las aplicaciones de FireAMP, ipbandeja.exe y agent.exe, se "procesen" mediante el Administrador de tareas de Windows.

Detención del servicio de conector de FireAMP

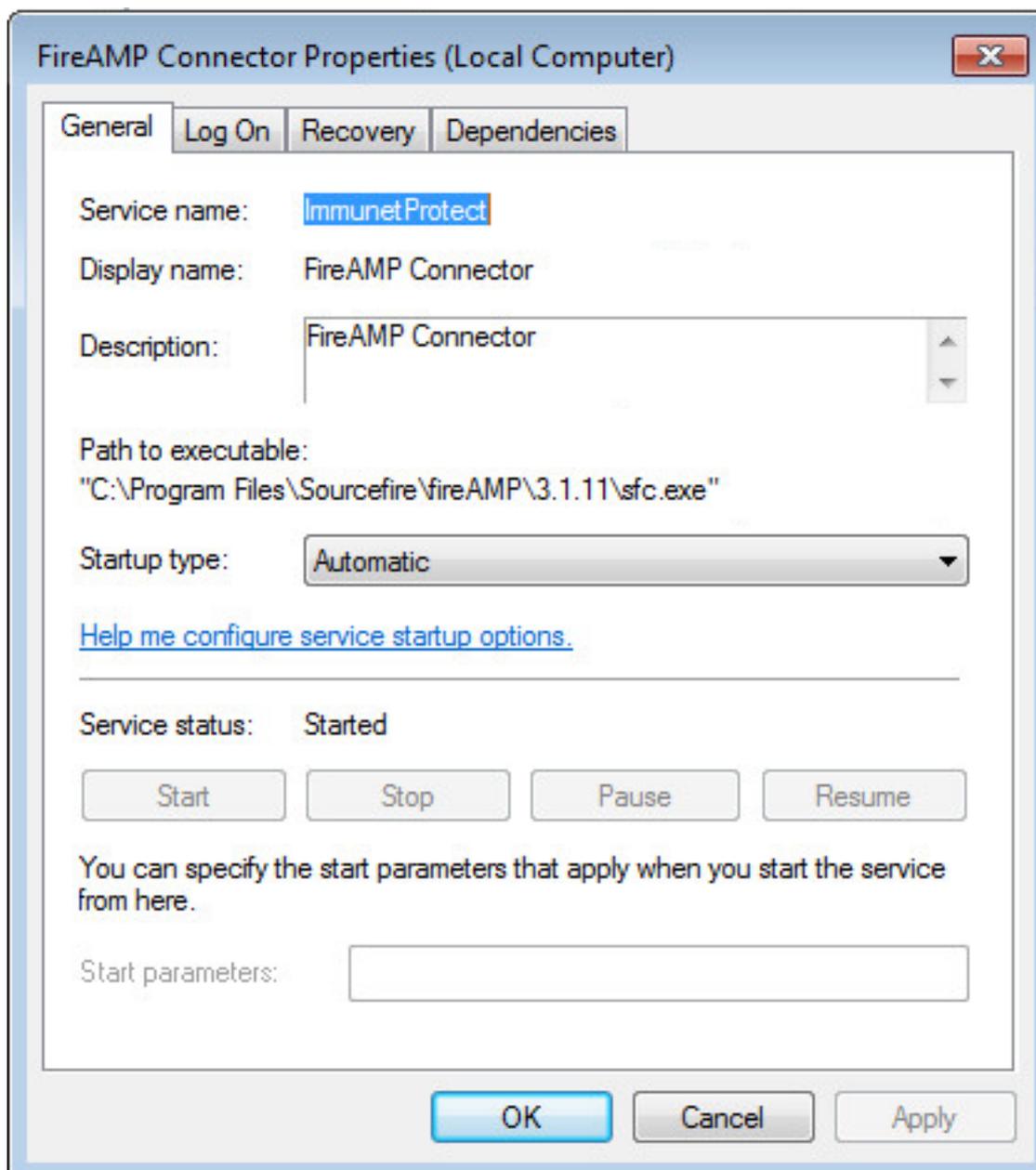
Razones para detener

Algunos escenarios en los que podría querer detener el servicio de conector de FireAMP o desinstalar FireAMP serían:

1. Detenga el servicio para quitar los archivos de base de datos dañados o los archivos de registro antiguos.
2. Desinstale FireAMP debido a un error, una instalación dañada o incompleta.
3. Reemplace el archivo policy.xml para diagnosticar problemas de conectividad.

Detener servicio mediante propiedades del conector

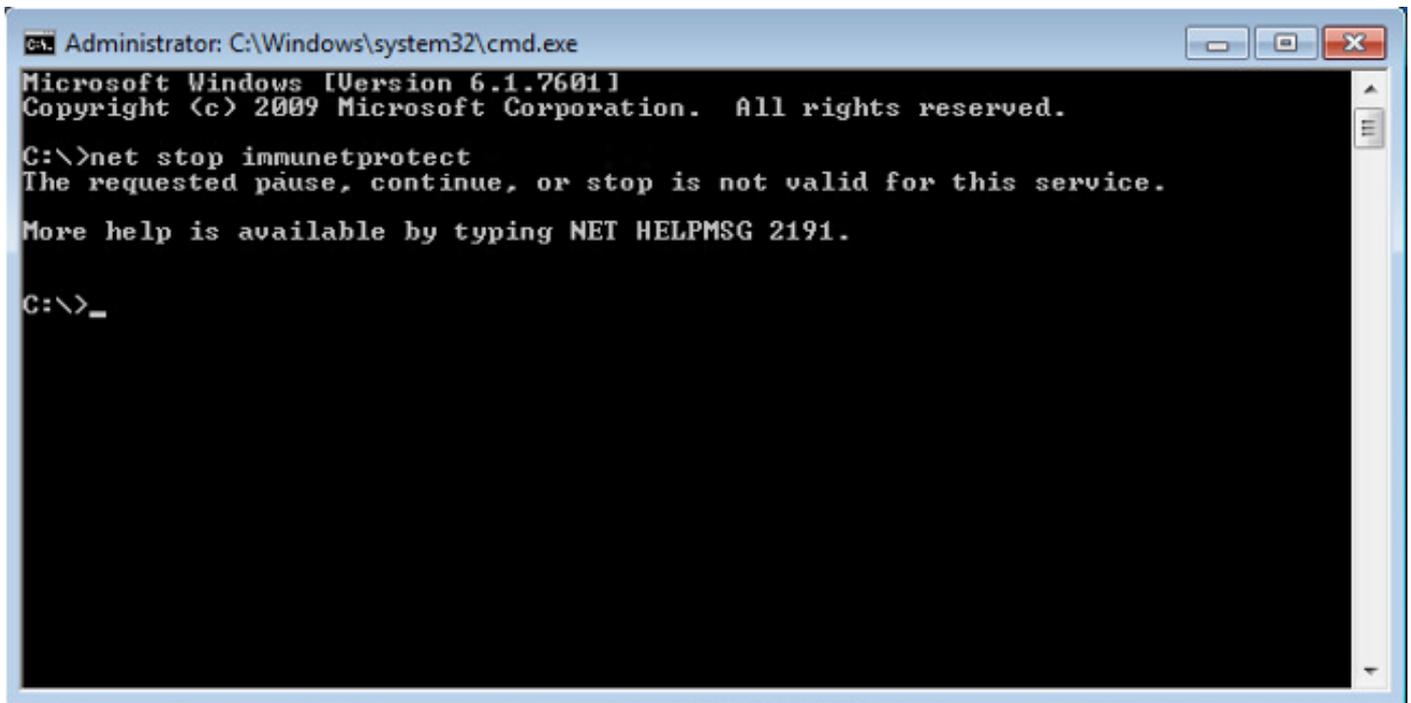
No podrá detener el servicio mediante la ventana **Propiedades del conector de FireAMP** si la **función Protección del conector** está habilitada. Los botones para administrar el servicio están desactivados como se indica a continuación:



Detener servicio mediante CLI

Cuando intenta detener un servicio mientras la función de protección del conector está activada, recibe un mensaje de error como el siguiente:

```
The requested pause, continue, or stop is not valid for this service.
```

A screenshot of a Windows command prompt window. The title bar reads "Administrator: C:\Windows\system32\cmd.exe". The window content shows the following text:

```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\>net stop immunetprotect
The requested pause, continue, or stop is not valid for this service.
More help is available by typing NET HELPMSG 2191.

C:\>_
```

En la versión 4.3.0+, el servicio sfc.exe se puede detener con el comando "sfc.exe -k password", donde 'password' es la contraseña definida en la política.

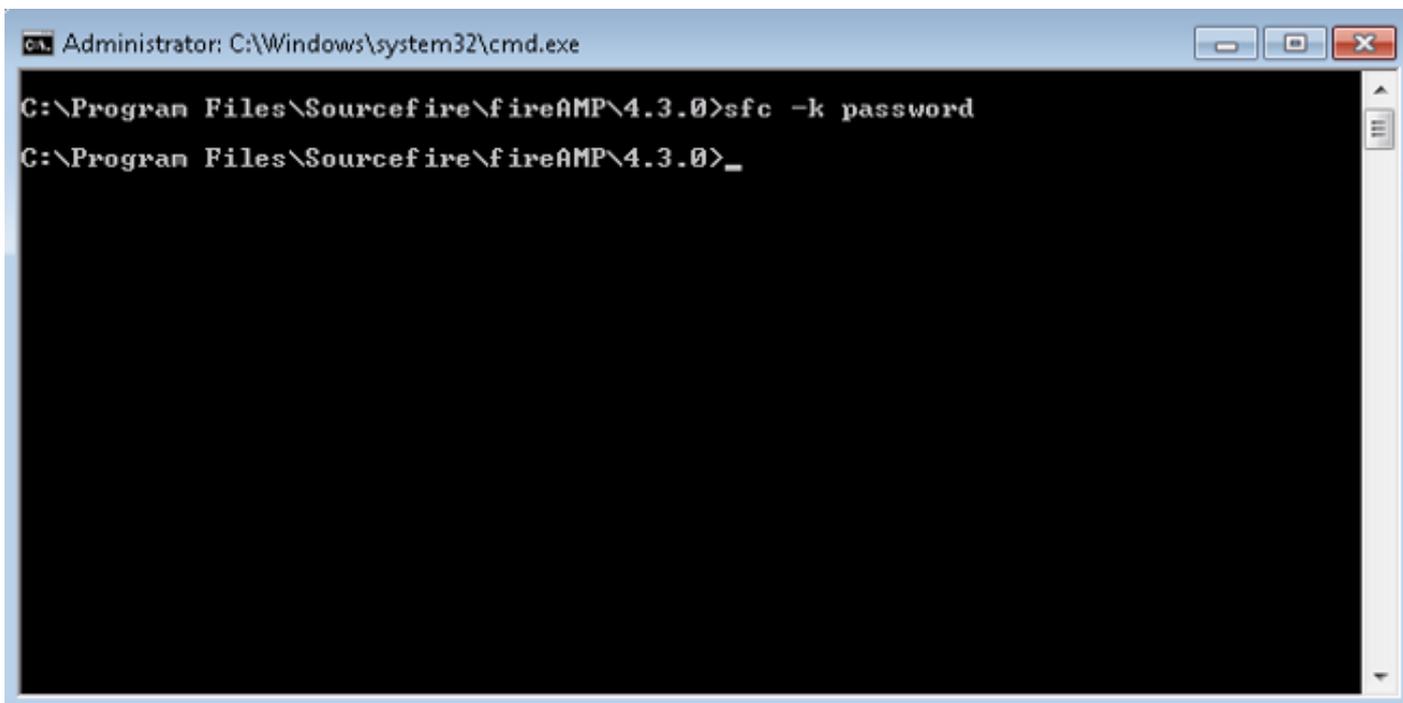
Solución

Detenga el servicio mediante la línea de comandos

Nota: Este comando sólo funciona en la versión 4.3.0 y superiores del conector FireAMP.

```
sfc.exe -k password
```

Reemplace la palabra "password" (contraseña) por la contraseña real establecida en su política.



```
Administrator: C:\Windows\system32\cmd.exe
C:\Program Files\Sourcefire\fireAMP\4.3.0>sfc -k password
C:\Program Files\Sourcefire\fireAMP\4.3.0>_
```

Detener servicio mediante la interfaz de usuario

Puede detener el servicio protegido mediante contraseña desde la interfaz de usuario.

