

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

Contenido

[Introducción](#)

[Configuración de la protección del conector](#)

[Driver de la autoprotección](#)

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

[Razones de una parada](#)

[Pare el servicio usando las propiedades del conector](#)

[Pare el servicio usando el CLI](#)

[Solución](#)

[Pare el servicio usando la línea de comando](#)

[Pare el servicio usando la interfaz de usuario](#)

Introducción

El conector de FireAMP tiene una característica llamada **Connector Protection**. Esta opción le permite a la contraseña proteger el servicio del conector de FireAMP y evita que sea parado o que desinstalado. Sin embargo, puede afectar el proceso de Troubleshooting debido al hecho de que la detención del servicio del conector de FireAMP o desinstalarlo puede venir adentro jugar como paso de Troubleshooting. Este documento describe cómo desinstalar FireAMP cuando es contraseña protegida.

Configuración de la protección del conector

Para habilitar la opción de protección del conector, edite su directiva, vaya a la **ficha general**, y amplíe las **características administrativas**.

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	

Driver de la autoprotección

La función de telefonía del conector utiliza un driver de la autoprotección para proteger los directorios para FireAMP. Un driver de la autoprotección realiza las tareas siguientes:

1. Proteja las claves de registro que FireAMP utiliza de ser borrado y modificación.
2. Proteja las aplicaciones contra la escritura o los archivos el borrar en el directorio de instalación. El directorio de instalación predeterminada es:

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

3. Proteja los drivers de FireAMP contra la descarga o el ser sobregrabado.
4. Proteja las aplicaciones de FireAMP, `iptray.exe` y `agent.exe`, contra ser "extremo procesado" vía el administrador de tareas de Windows.

Detención del servicio del conector de FireAMP

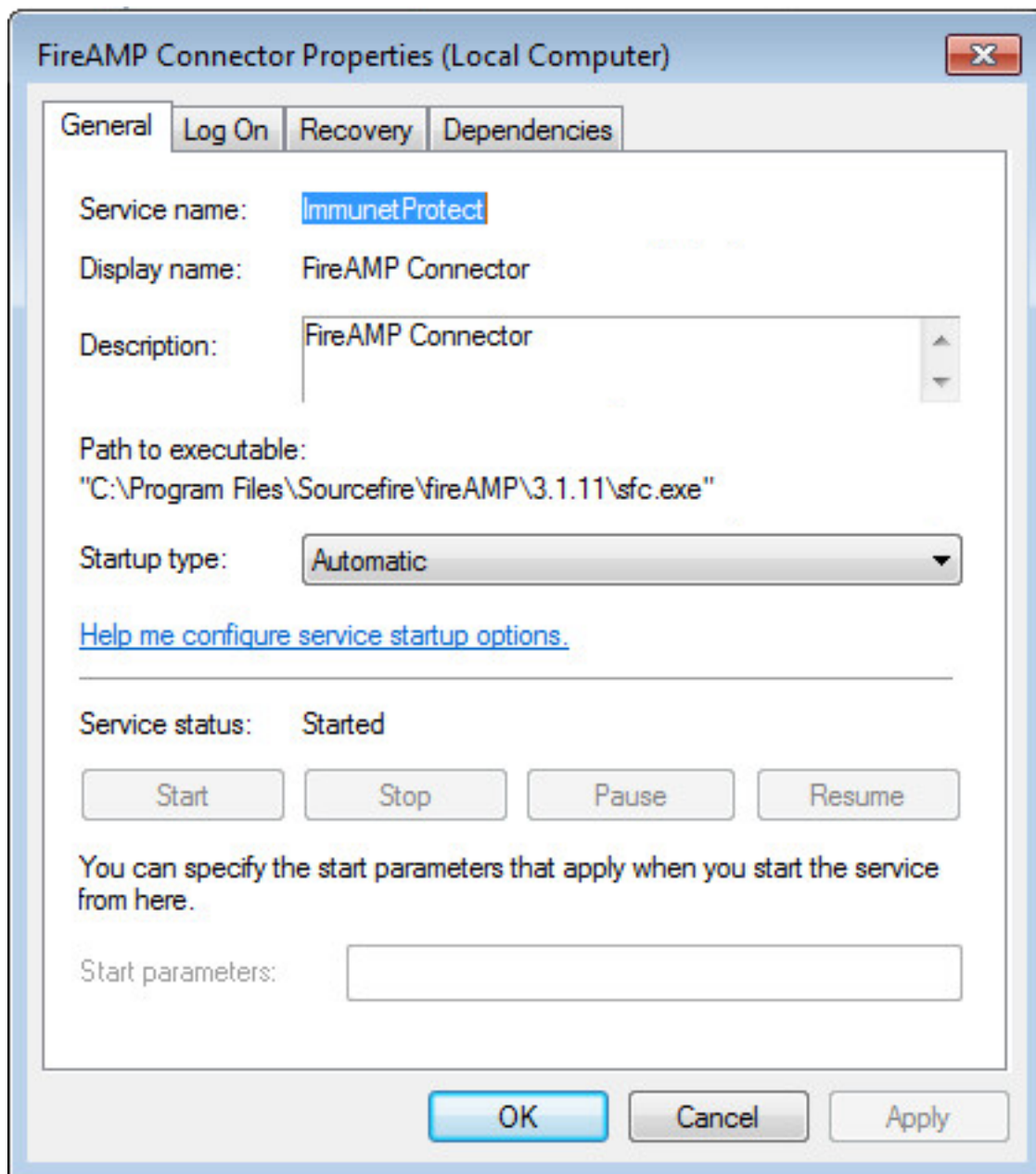
Razones de una parada

Algunos escenarios donde usted puede querer parar el servicio o la desinstalación FireAMP del conector de FireAMP estarían:

1. Pare el servicio para quitar los archivos de Base de datos dañada, o los viejos archivos del registro.
2. Desinstale FireAMP debido a un error, corrupto, o a la instalación incompleta.
3. Substituya el archivo `policy.xml` para diagnosticar los problemas de conectividad.

Pare el servicio usando las propiedades del conector

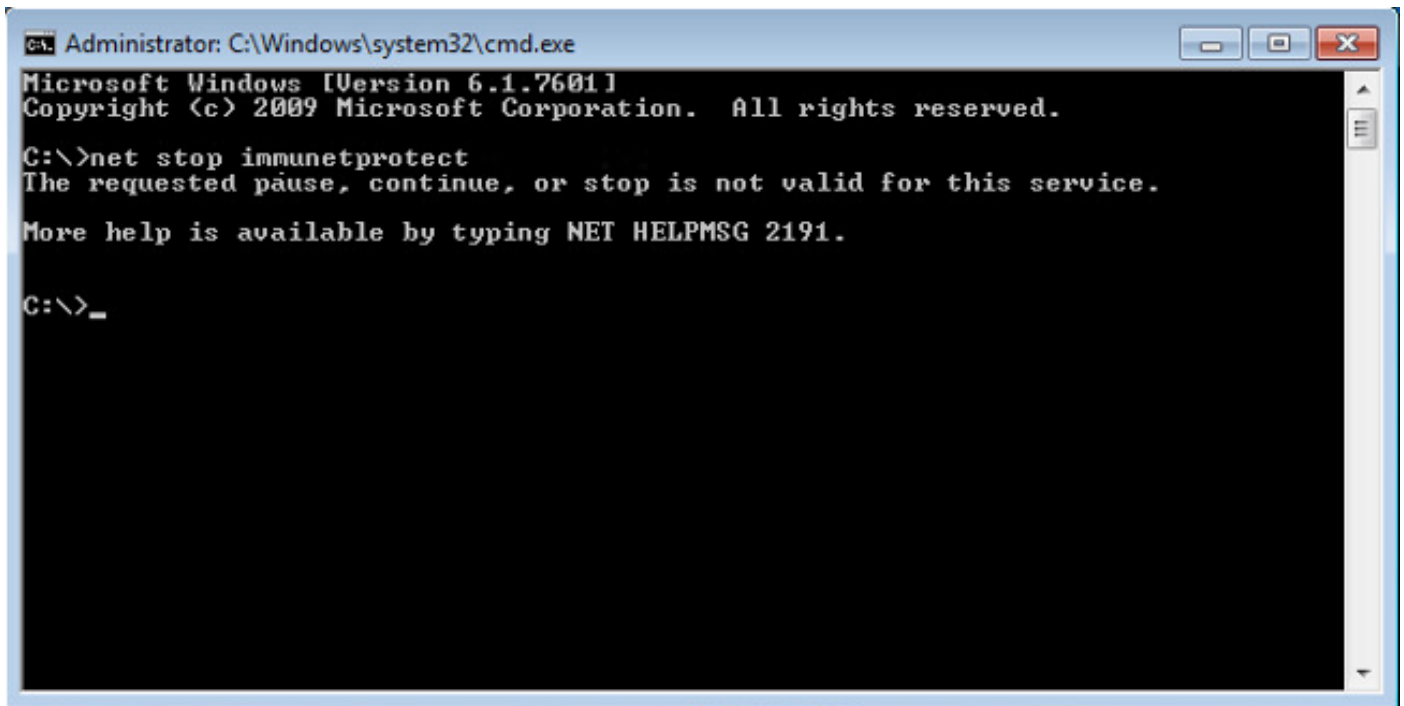
Usted no podrá parar el servicio usando la **ventana de pPropiedades del conector de FireAMP** si se habilita la **función de telefonía del conector**. Los botones para manejar el servicio se inhabilitan como abajo:



Pare el servicio usando el CLI

Quando usted intenta parar un servicio mientras que se habilita la función de telefonía del conector, usted recibe un mensaje de error como abajo:

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



```
Administrator: C:\Windows\system32\cmd.exe
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 parar con el comando “sfc.exe - contraseña k” donde está la contraseña la “contraseña” definida en la directiva.

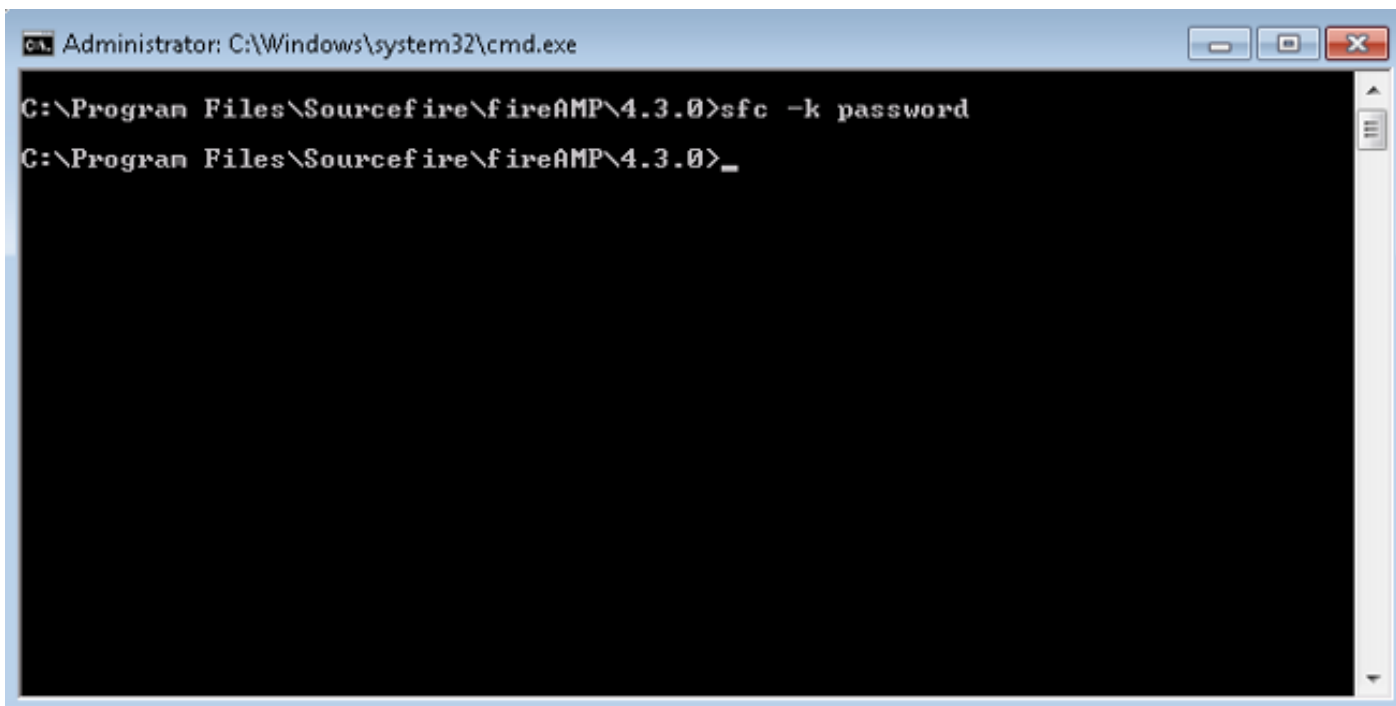
Solución

Pare el servicio usando la línea de comando

Nota - Este comando trabaja solamente en la versión 4.3.0 y posterior del conector de FireAMP.

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

Substituya la palabra “contraseña” por la contraseña definida real en su directiva.



```
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>_
```

Pare el servicio usando la interfaz de usuario

Usted puede parar el servicio protegido contraseña de la interfaz de usuario.

