

커넥터 보호 때문에 FireAMP Connector 서비스를 중지하지 못함

목차

[소개](#)

[커넥터 보호 구성](#)

[자체 보호 드라이버](#)

[FireAMP Connector 서비스 중지](#)

[중지 사유](#)

[커넥터 속성을 사용하여 서비스 중지](#)

[CLI를 사용하여 서비스 중지](#)

[솔루션](#)

[명령줄을 사용하여 서비스 중지](#)

[사용자 인터페이스를 사용하여 서비스 중지](#)

소개

FireAMP Connector에는 Connector **Protection**이라는 기능이 있습니다. 이 옵션을 사용하면 FireAMP Connector 서비스를 암호로 보호하여 이를 중지하거나 제거할 수 있습니다. 그러나 FireAMP 커넥터 서비스를 중지하거나 제거하는 것이 트러블슈팅 단계로 작동하기 위해 들어올 수 있기 때문에 트러블슈팅 프로세스에 영향을 미칠 수 있습니다. 이 문서에서는 FireAMP가 비밀번호로 보호될 때 제거하는 방법에 대해 설명합니다.

커넥터 보호 구성

커넥터 보호 옵션을 활성화하려면 **정책**을 편집하고 **일반 탭**으로 이동한 다음 **관리 기능을 확장**합니다.

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	

자체 보호 드라이버

Connector Protection 기능은 자체 보호 드라이버를 사용하여 FireAMP용 디렉토리를 보호합니다. 자체 보호 드라이버는 다음 작업을 수행합니다.

1. FireAMP에서 사용하는 레지스트리 키를 삭제 및 수정하지 못하도록 보호합니다.
2. 응용 프로그램이 설치 디렉터리에 파일을 쓰거나 삭제하지 못하도록 보호합니다. 기본 설치 디렉토리는 다음과 같습니다.

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

3. FireAMP 드라이버를 언로드하거나 덮어쓰지 않도록 보호합니다.
4. Windows 작업 관리자를 통해 FireAMP 애플리케이션, iptray.exe 및 agent.exe를 "End Processed"에서 보호합니다.

FireAMP Connector 서비스 중지

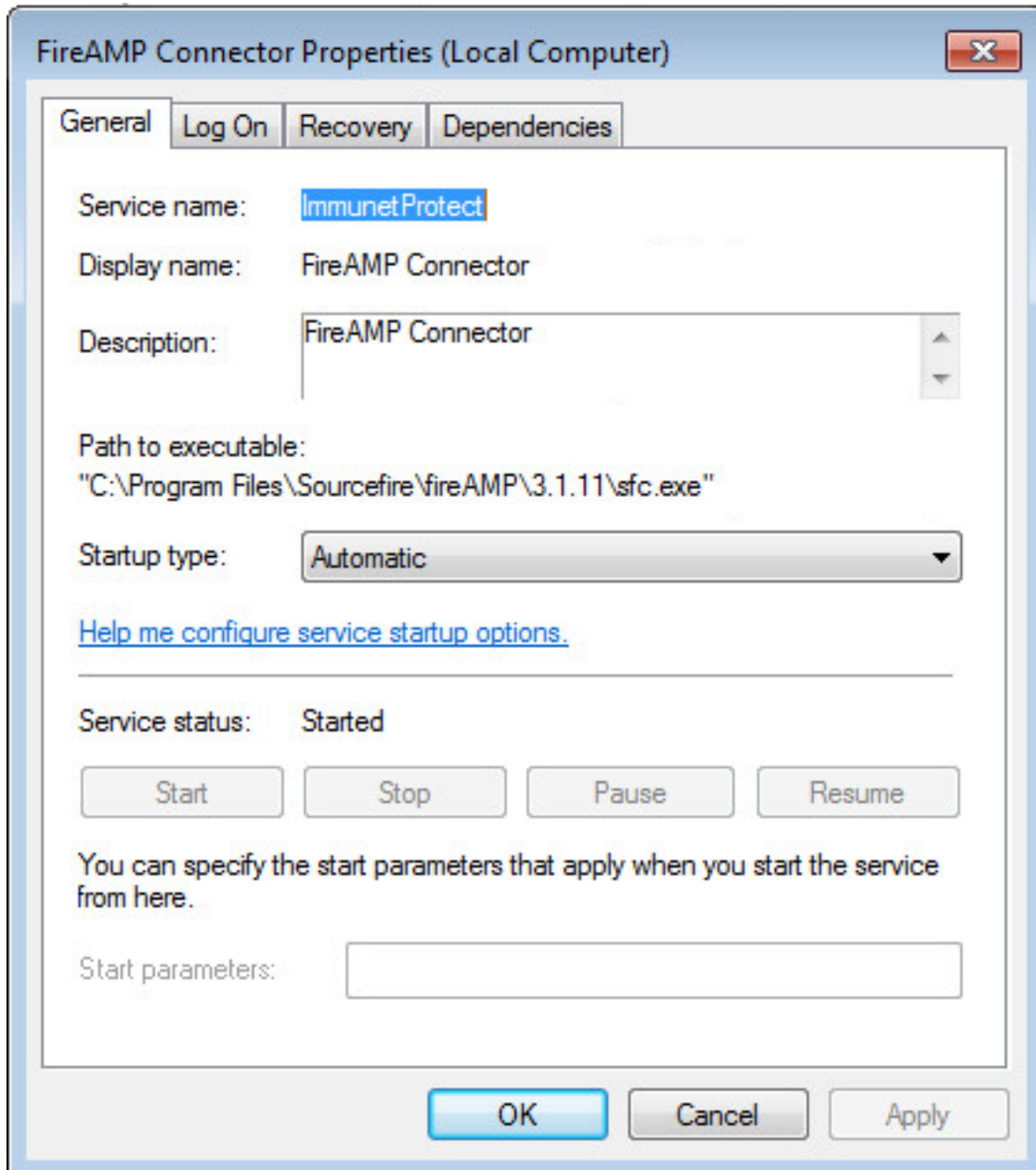
중지 사유

FireAMP 커넥터 서비스를 중지하거나 FireAMP를 제거할 수 있는 몇 가지 시나리오는 다음과 같습니다.

1. 손상된 데이터베이스 파일 또는 이전 로그 파일을 제거하려면 서비스를 중지합니다.
2. 오류, 손상 또는 불완전한 설치로 인해 FireAMP를 제거합니다.
3. 연결 문제를 진단하려면 policy.xml 파일을 교체합니다.

커넥터 속성을 사용하여 서비스 중지

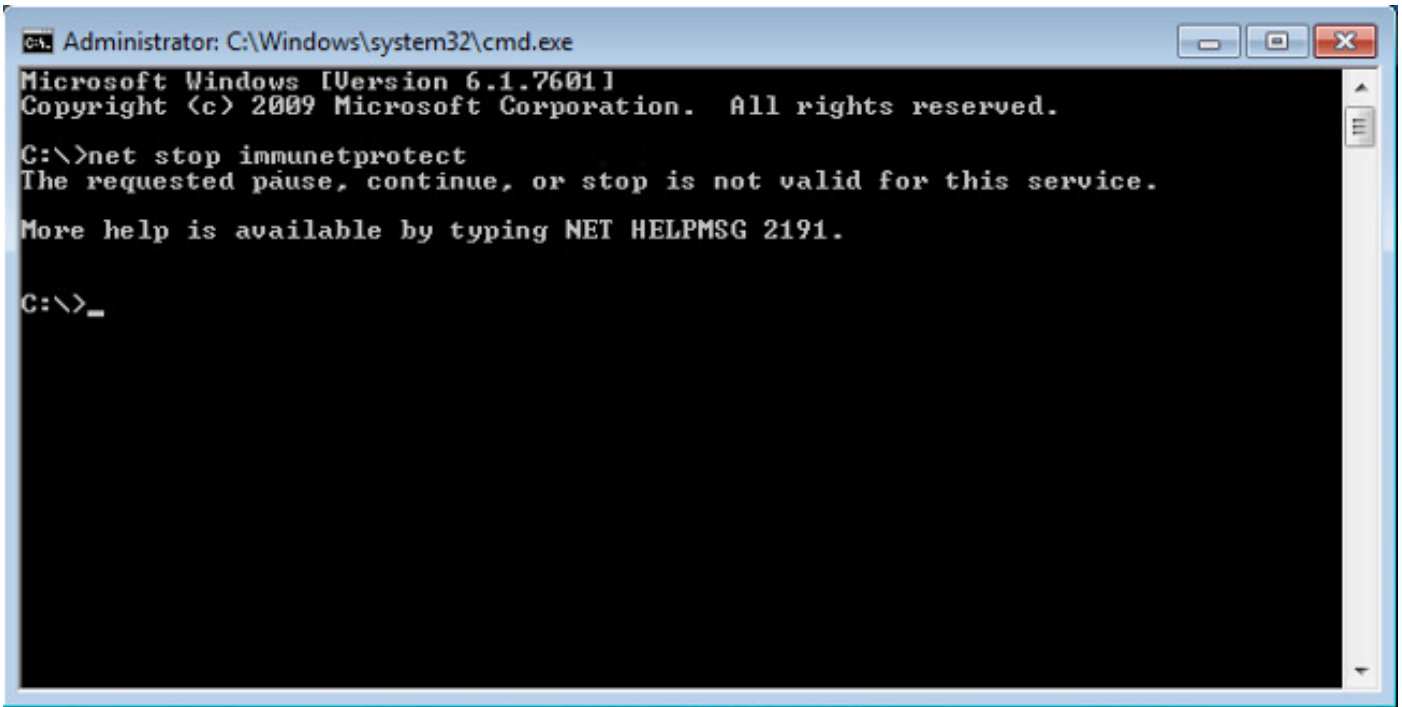
Connector Protection 기능이 활성화된 경우 FireAMP Connector Properties 창을 사용하여 서비스를 중지할 수 없습니다. 서비스를 관리하는 버튼은 아래와 같이 비활성화됩니다.



CLI를 사용하여 서비스 중지

커넥터 보호 기능이 활성화된 상태에서 서비스를 중지하려고 하면 다음과 같은 오류 메시지가 표시 됩니다.

```
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:\>_
```

버전 4.3.0+에서 sfc.exe 서비스는 "sfc.exe -k password" 명령을 사용하여 중지할 수 있습니다. 여기서 'password'는 정책에 정의된 암호입니다.

솔루션

명령줄을 사용하여 서비스 중지

참고 - 이 명령은 FireAMP Connector 버전 4.3.0 이상에서만 작동합니다.

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

"password"라는 단어를 정책에 설정된 실제 비밀번호로 바꿉니다.

```
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>_
```

사용자 인터페이스를 사용하여 서비스 중지

사용자 인터페이스에서 비밀번호 보호 서비스를 중지할 수 있습니다.

