FireAMP Connector-Dienst wird wegen Verbindungsschutz nicht angehalten

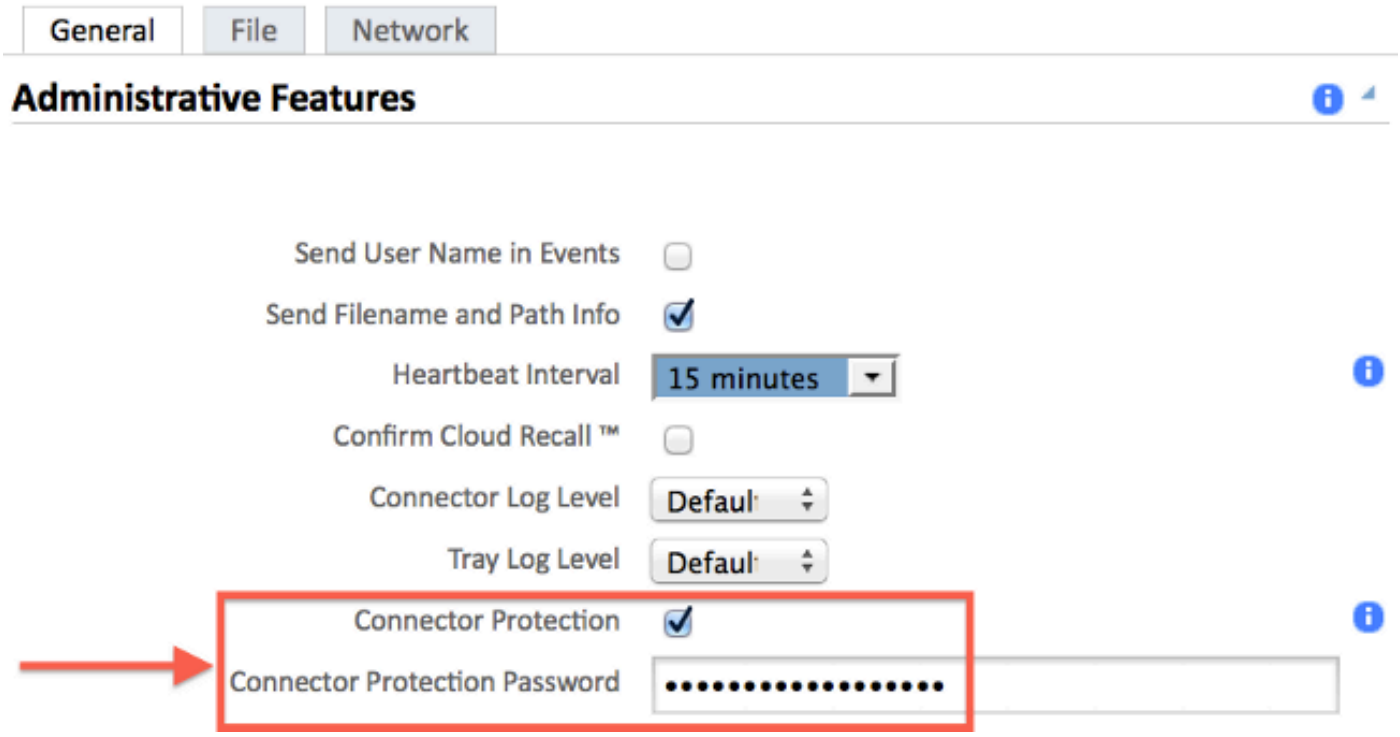
Inhalt

Einführung

Der FireAMP Connector verfügt über eine Funktion namens **Connector Protection**. Mit dieser Option können Sie den FireAMP Connector-Dienst durch ein Kennwort schützen und verhindern, dass er beendet oder deinstalliert wird. Dies kann sich jedoch auf die Fehlerbehebung auswirken, da das Beenden des FireAMP-Connector-Dienstes oder die Deinstallation dieses Dienstes als Fehlerbehebungsschritt eintreten kann. In diesem Dokument wird beschrieben, wie FireAMP deinstalliert wird, wenn es kennwortgeschützt ist.

Konfiguration des Connector-Schutzes

Um die Option **Connector Protection** zu aktivieren, bearbeiten Sie Ihre **Richtlinie**, gehen Sie zur **Registerkarte General** (Allgemein), und erweitern Sie **Administrative Features (Verwaltungsfunktionen)**.



Self-Protect-Treiber

Die Connector Protection-Funktion nutzt einen selbstsichernden Treiber, um die Verzeichnisse für FireAMP zu schützen. Ein Selbstschutztreiber führt die folgenden Aufgaben aus:

1. Von FireAMP verwendete Registrierungsschlüssel können nicht gelöscht und geändert werden.
2. Schützen Sie Anwendungen vor dem Schreiben oder Löschen von Dateien im Installationsverzeichnis. Das Standardinstallationsverzeichnis ist:

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

3. Schützen Sie die FireAMP-Treiber vor dem Entladen oder Überschreiben.
4. Schützen Sie FireAMP-Anwendungen, iptray.exe und agent.exe, davor, mithilfe des Windows Task-Managers "End Processing" zu sein.

Beenden des FireAMP Connector-Service

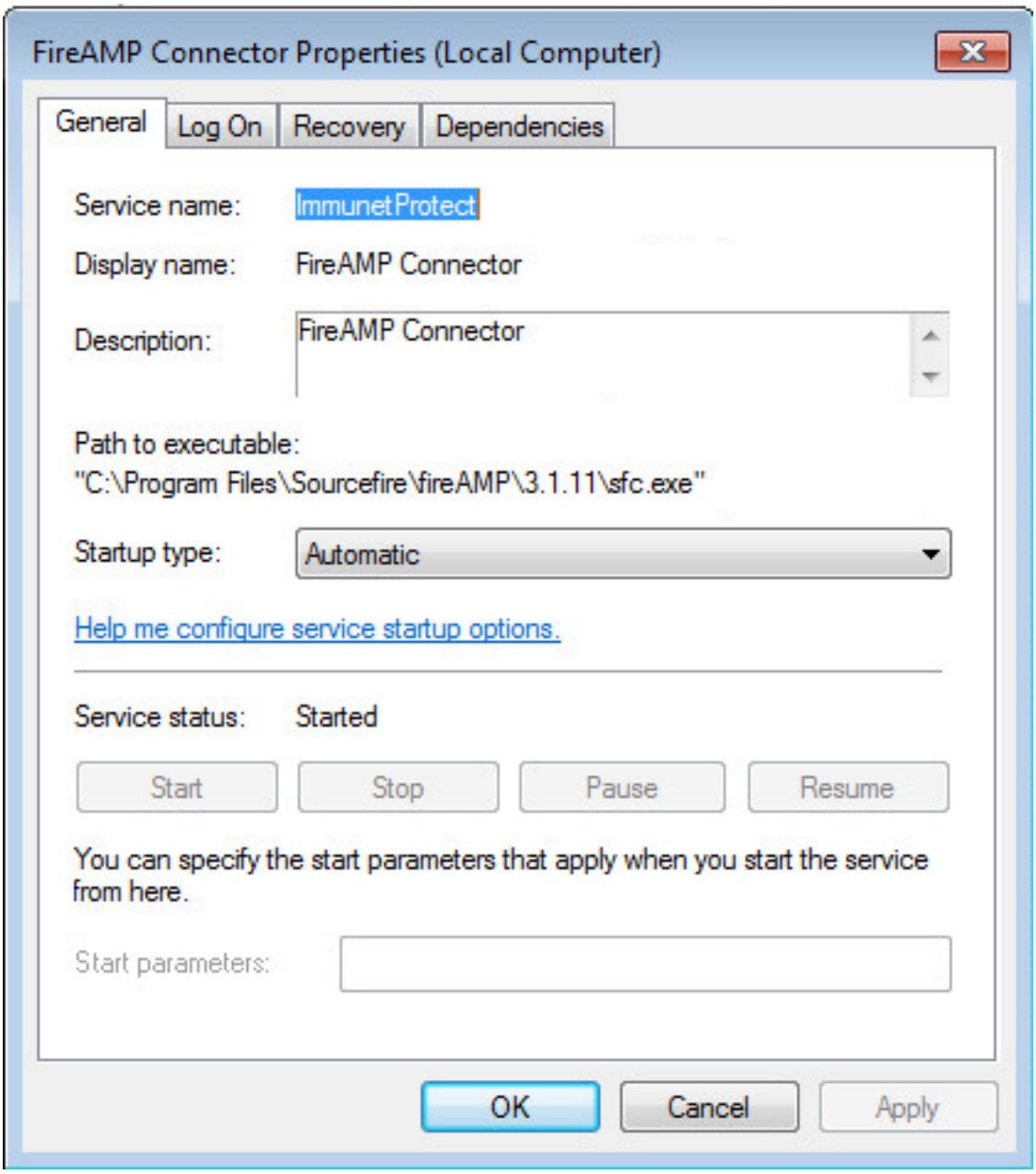
Gründe für einen Stopp

Einige Szenarien, in denen Sie den FireAMP-Connector-Dienst beenden oder FireAMP deinstallieren möchten, sind:

1. Beenden Sie den Dienst, um beschädigte Datenbankdateien oder alte Protokolldateien zu entfernen.
2. Deinstallieren Sie FireAMP aufgrund einer fehlerhaften, beschädigten oder unvollständigen Installation.
3. Ersetzen Sie die Datei policy.xml, um Verbindungsprobleme zu diagnostizieren.

Dienst mit Verbindungseigenschaften beenden

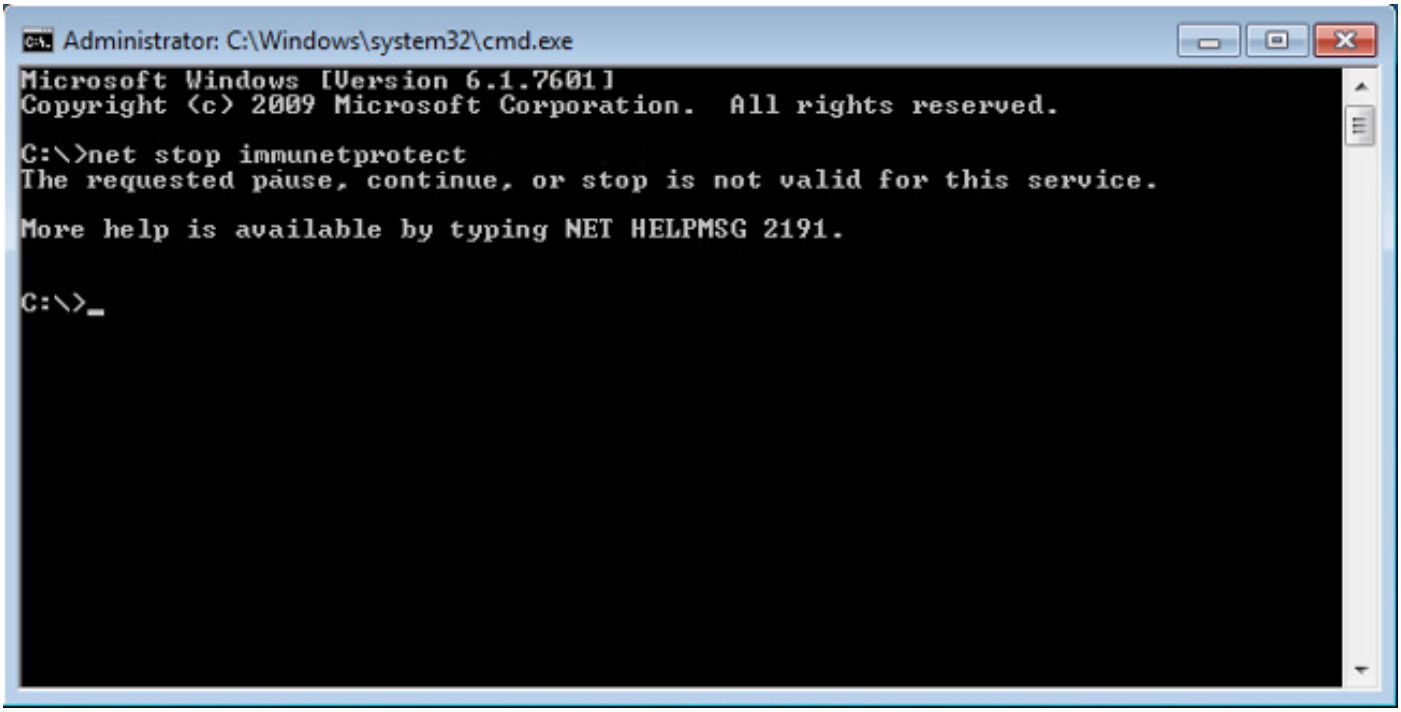
Sie können den Dienst nicht über das Fenster **Eigenschaften** des **FireAMP Connectors** beenden, wenn die Funktion **Connector Protection** aktiviert ist. Die Tasten zum Verwalten des Service sind wie folgt deaktiviert:



Dienst über CLI beenden

Wenn Sie versuchen, einen Dienst zu beenden, während die Verbindungsschutzfunktion aktiviert ist, erhalten Sie eine Fehlermeldung wie folgt:

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



In Version 4.3.0+ kann der Dienst sfc.exe mit dem Befehl "sfc.exe -k password" beendet werden, wobei "password" das in der Richtlinie definierte Kennwort ist.

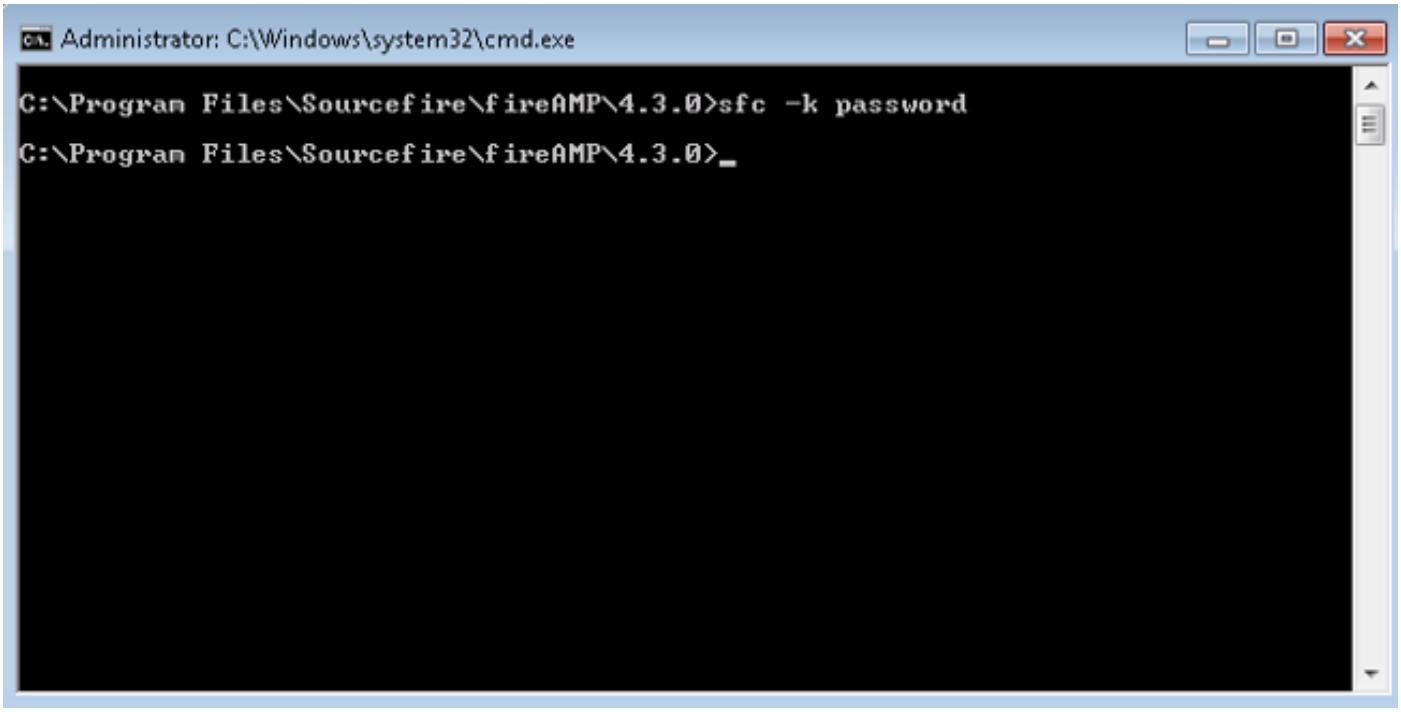
Lösung

Beenden Sie den Dienst über die Befehlszeile.

Hinweis: Dieser Befehl funktioniert nur mit Version 4.3.0 und höher des FireAMP Connectors.

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

Ersetzen Sie das Wort "password" durch das in Ihrer Richtlinie festgelegte eigentliche Kennwort.



Dienst über die Benutzeroberfläche beenden

Sie können den kennwortgeschützten Dienst über die Benutzeroberfläche beenden.