De FirePOWER-connector kan niet stoppen door beveiliging van de connector

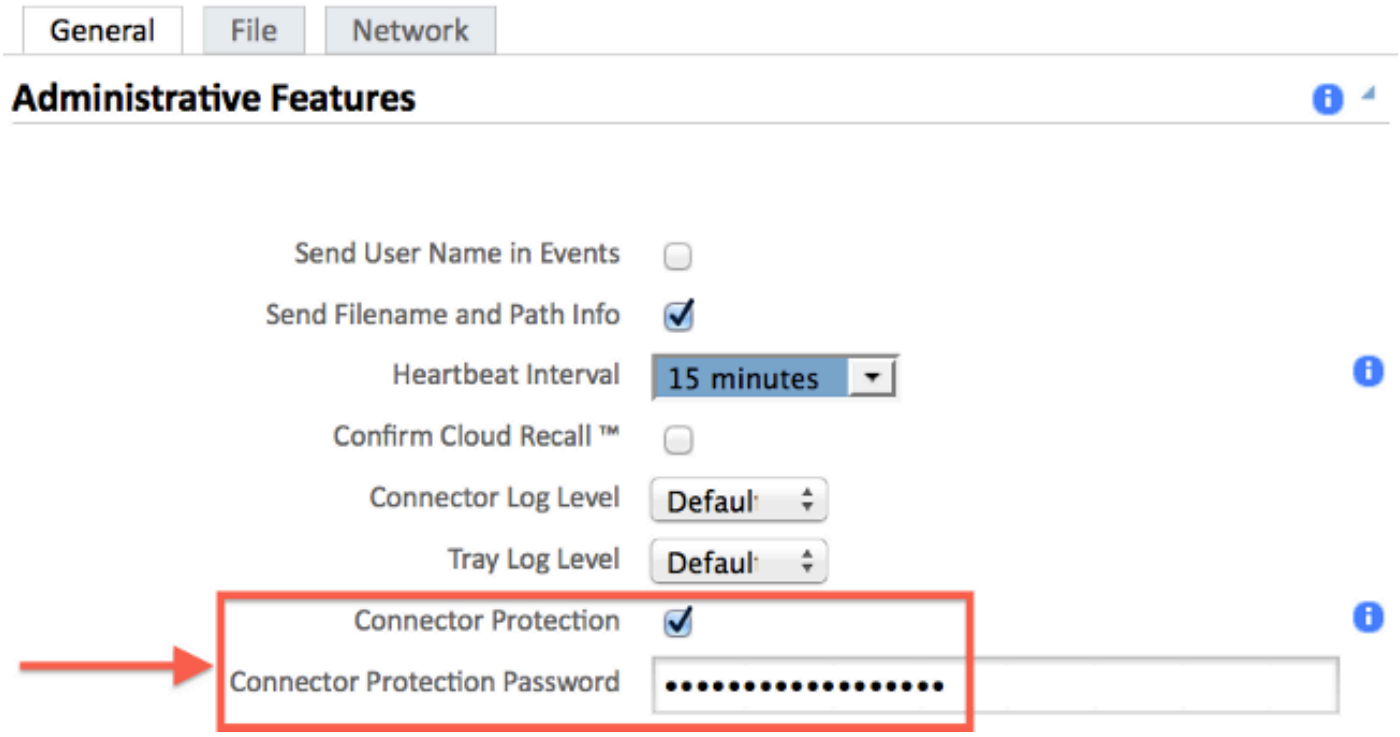
Inhoud

Inleiding

De FireAMP-connector heeft een functie die **Connectorbescherming** heet. Met deze optie kunt u de FireAMP-connector beveiligen en voorkomen dat deze wordt stopgezet of niet geïnstalleerd. Dit kan echter gevolgen hebben voor het proces voor het oplossen van problemen doordat het stoppen van de FireAMP-connector of het verwijderen van de software kan worden ingevoerd als een stap voor het oplossen van problemen. Dit document beschrijft hoe u FireAMP kunt verwijderen wanneer dit met een wachtwoord is beveiligd.

Configuratie van de connector

Bewerk de optie **Bescherming** van de **connector** als u dit **beleid wilt** inschakelen, ga naar het **tabblad Algemeen** en breder **beheerfuncties**.



zelfbeschermer

Connectorbescherming maakt gebruik van een zelfbeveiligingsstuurprogramma om de directories voor FireAMP te beschermen. Een bestuurder die zichzelf beschermt voert de volgende taken uit:

1. Bescherm de registratiesleutels die FireAMP gebruikt om te voorkomen dat deze worden verwijderd en aangepast.
2. Beveiliging van toepassingen tegen het schrijven of verwijderen van bestanden in de installatiemap. De standaard installatiemap is:

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

3. Bescherm de FireAMP-stuurprogramma's tegen uitlading of overschreven.
4. Bescherm FireAMP-toepassingen, iptray.exe en agent.exe, tegen "End Processed" via Windows Task Manager.

FirePOWER-connector

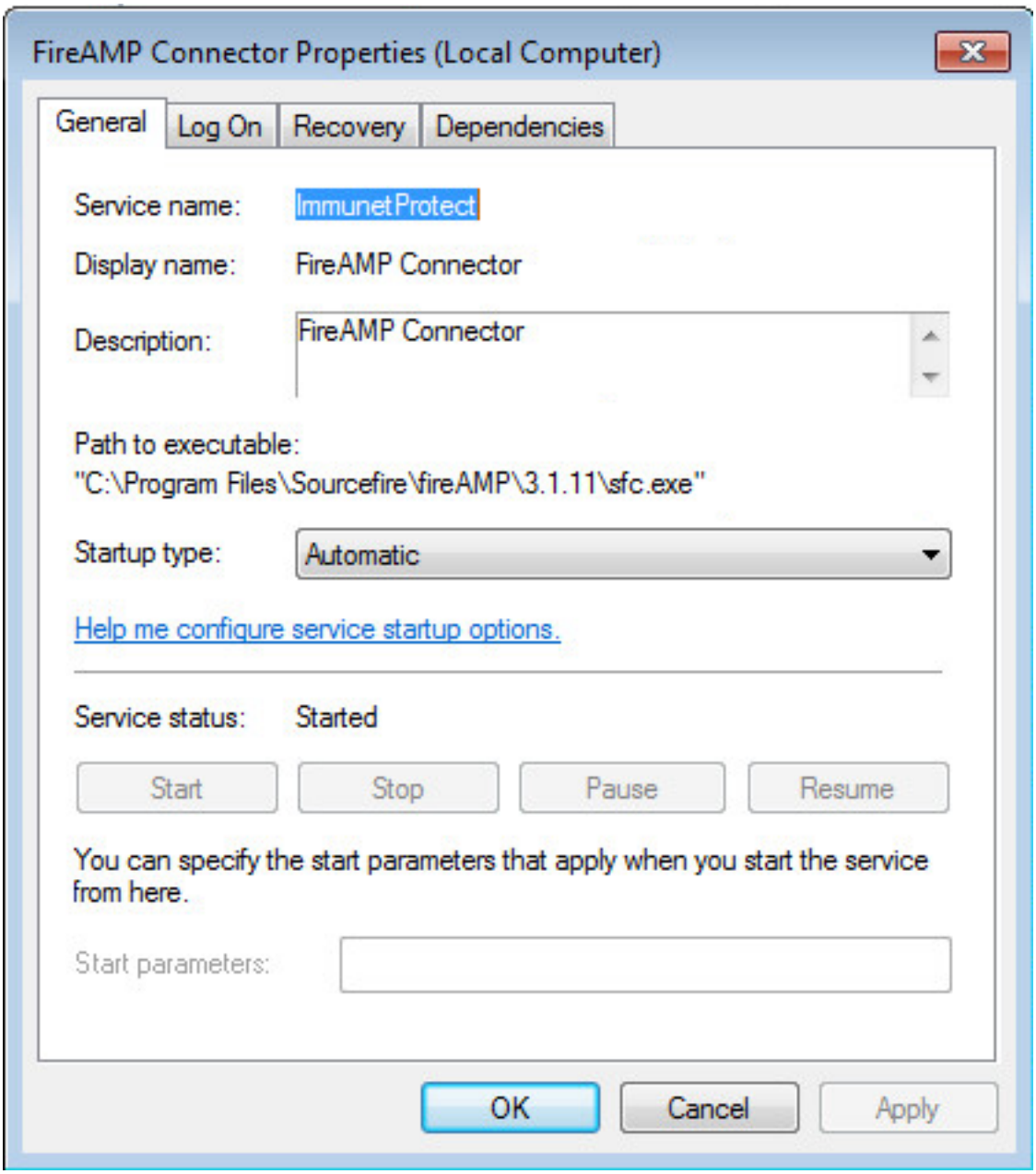
Redenen voor een halt

Sommige scenario's waarin u de FireAMP-connector wilt stoppen of FireAMP wilt verwijderen, zijn:

1. Stop de service om beschadigde databases of oude logbestanden te verwijderen.
2. Installeer FirePOWER niet vanwege een fout, beschadiging of onvolledige installatie.
3. Vervang het bestand policy.xml om problemen met de connectiviteit te diagnosticeren.

Service stoppen met behulp van connector-eigenschappen

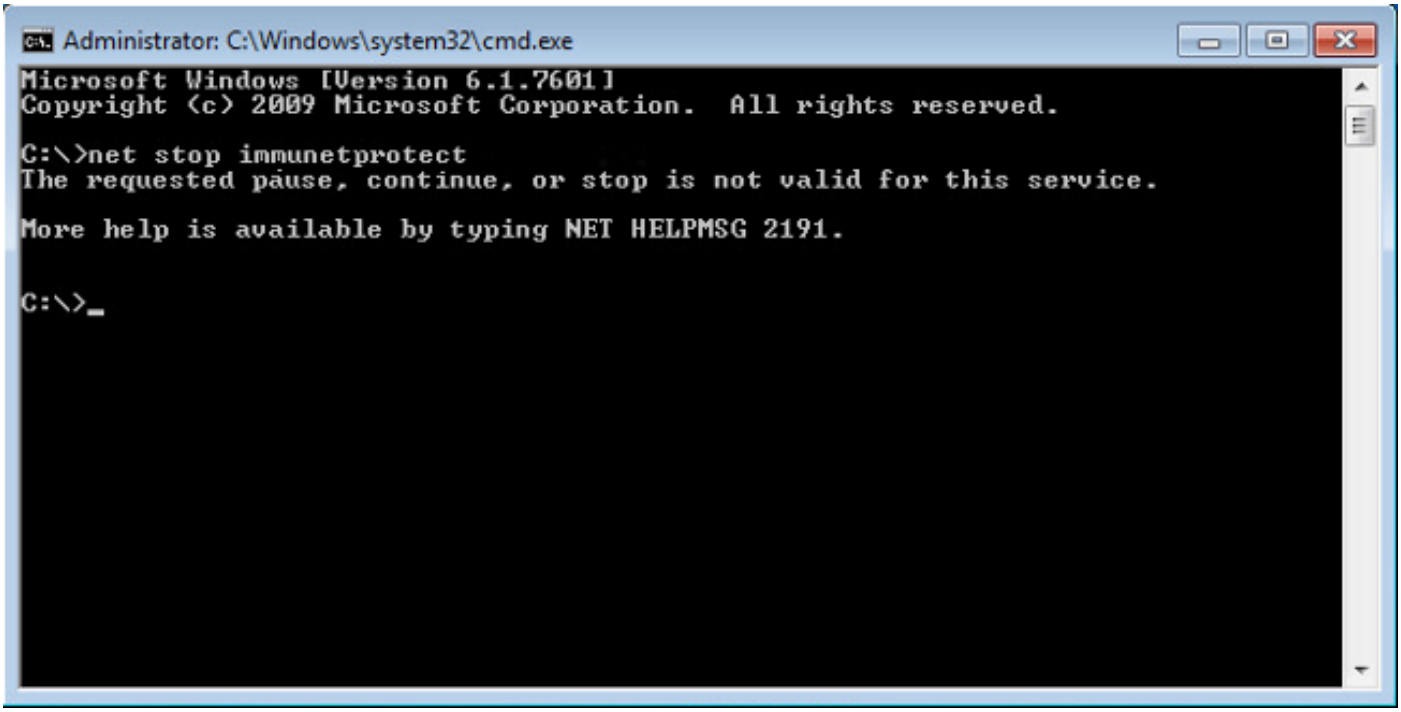
U kunt de service niet stoppen met behulp van het **venster** van de **FireAMP-connector** als de **connector** is ingeschakeld. De knoppen voor het beheer van de service zijn als volgt uitgeschakeld:



Service stoppen met CLI

Wanneer u probeert een service te stoppen terwijl de verbindingsbeveiligingsfunctie ingeschakeld is, ontvangt u zoals hieronder een melding van storing:

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



Op versie 4.3.0+ kan de dienst sfc.exe worden gestopt met de opdracht "sfc.exe -k wachtwoord" waarbij "wachtwoord" het wachtwoord is dat in het beleid is gedefinieerd.

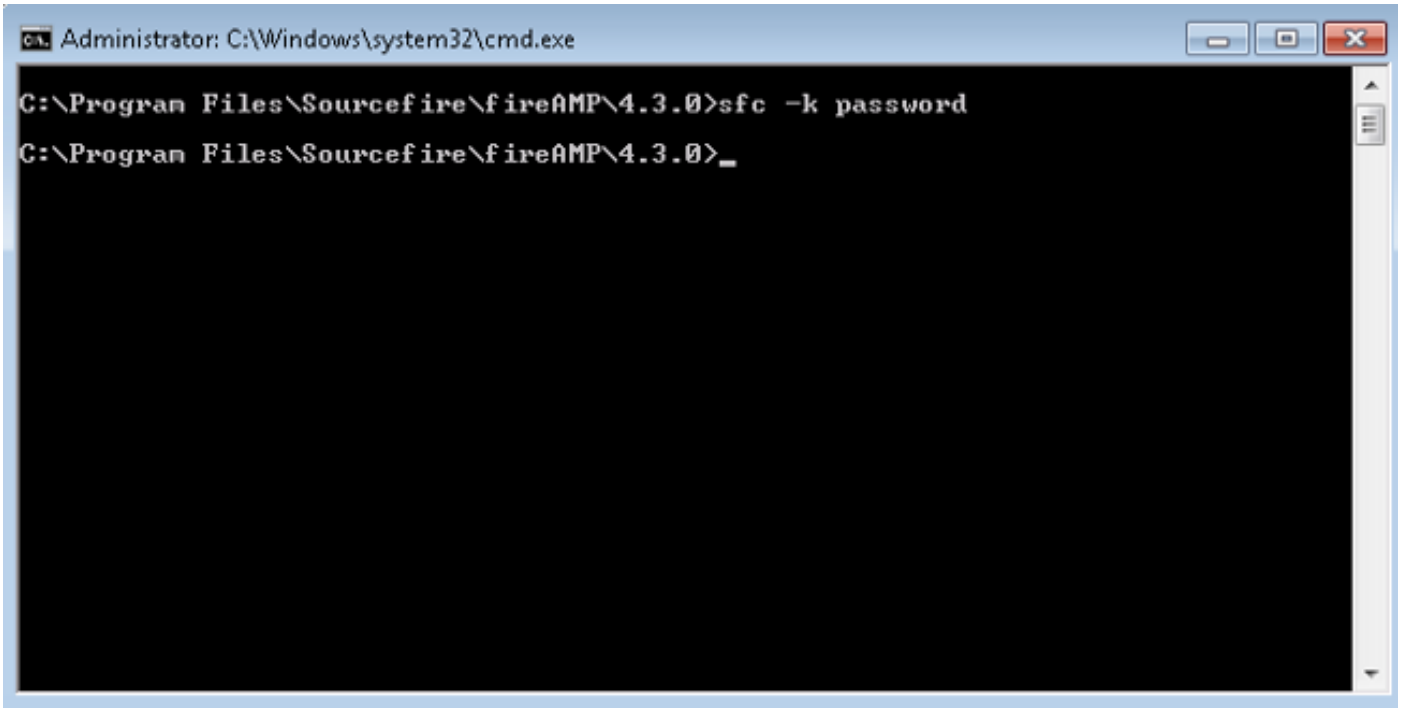
Oplossing

Stop de service met behulp van de opdrachtregel

Opmerking - Deze opdracht werkt alleen op versie 4.3.0 en hoger van de FireAMP-connector.

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

Vervang het woord "wachtwoord" door het wachtwoord dat in het beleid is ingesteld.



Service stoppen met gebruik van gebruikersinterface

U kunt de wachtwoordbeveiliging van de gebruikersinterface stoppen.