FireAMP聯結器服務因聯結器保護而無法停止

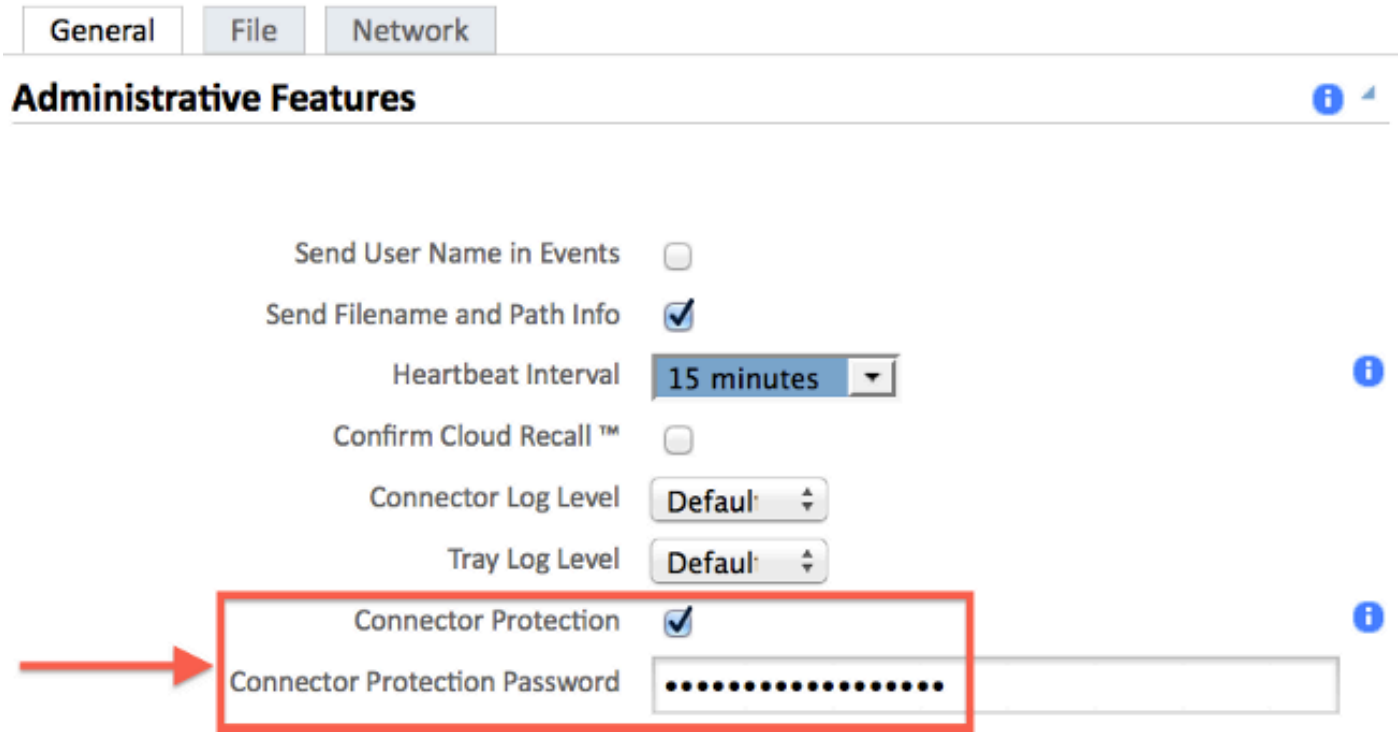
目錄

簡介

FireAMP聯結器具有稱為「聯結器保護」**的功能**。此選項允許您對FireAMP聯結器服務進行密碼保護，並防止停止或解除安裝該服務。但是，這可能會影響故障排除過程，因為停止FireAMP聯結器服務或解除安裝該聯結器服務可以作為故障排除步驟來進行。本文檔介紹如何在FireAMP受到密碼保護時將其解除安裝。

聯結器保護的配置

若要啟用Connector Protection選項，請編輯Policy，轉到General頁籤，然後展開Administrative Features。



自我保護驅動程式

聯結器保護功能利用自我保護驅動程式來保護FireAMP的目錄。自我保護驅動程式執行以下任務：

1. 保護FireAMP使用的登錄檔項不被刪除和修改。
2. 防止應用程式寫入或刪除安裝目錄中的檔案。預設安裝目錄為：

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

3. 防止FireAMP驅動程式被解除安裝或覆蓋。
4. 通過Windows工作管理員保護FireAMP應用程式iptray.exe和agent.exe，使其不受「最終處理」的影響。

停止FireAMP聯結器服務

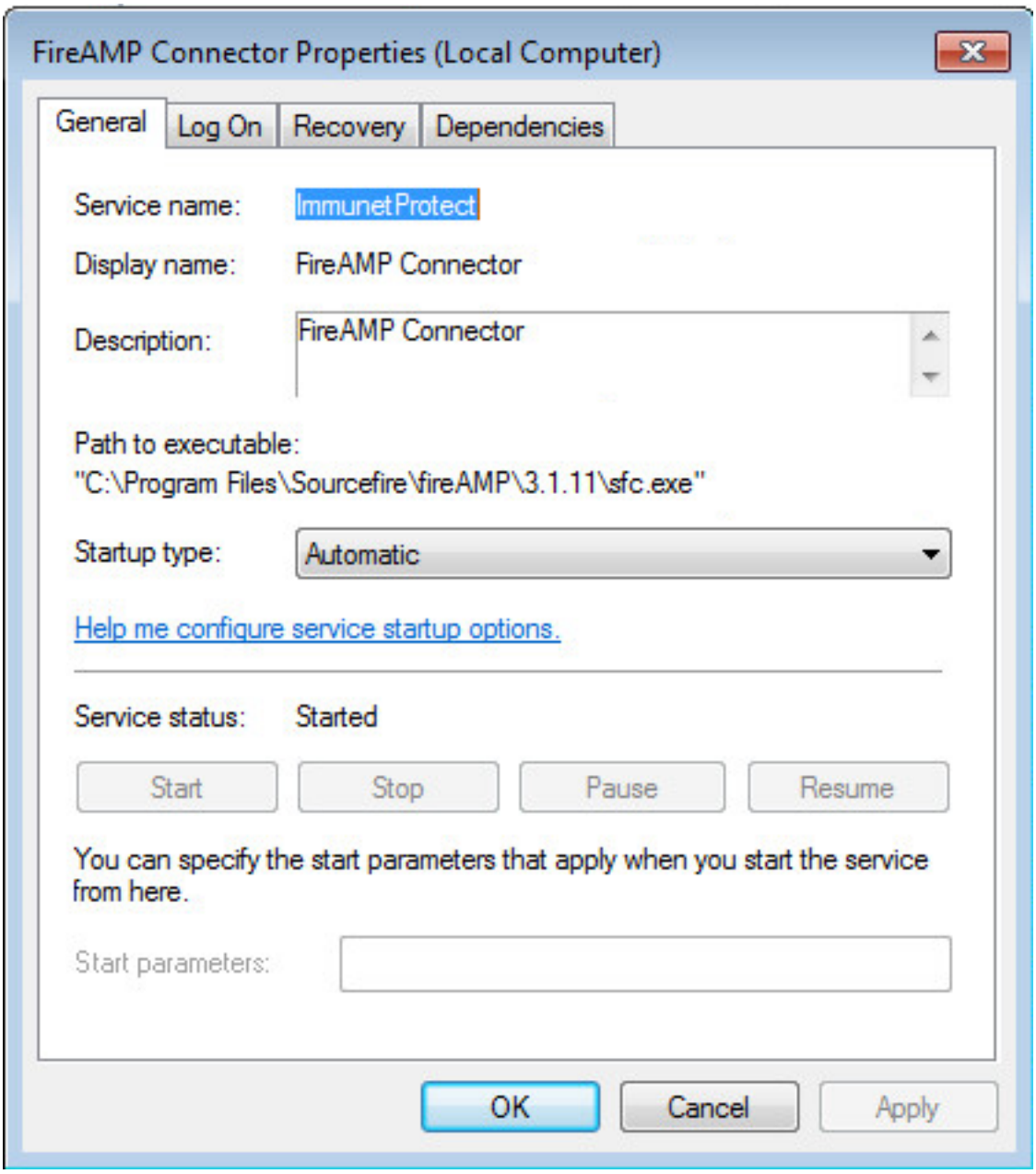
停止的原因

您可能希望停止FireAMP聯結器服務或解除安裝FireAMP的一些情況如下：

1. 停止該服務以刪除損壞的資料庫檔案或舊日誌檔案。
2. 由於錯誤、損壞或不完整的安裝而解除安裝FireAMP。
3. 替換policy.xml檔案以診斷連線問題。

使用聯結器屬性停止服務

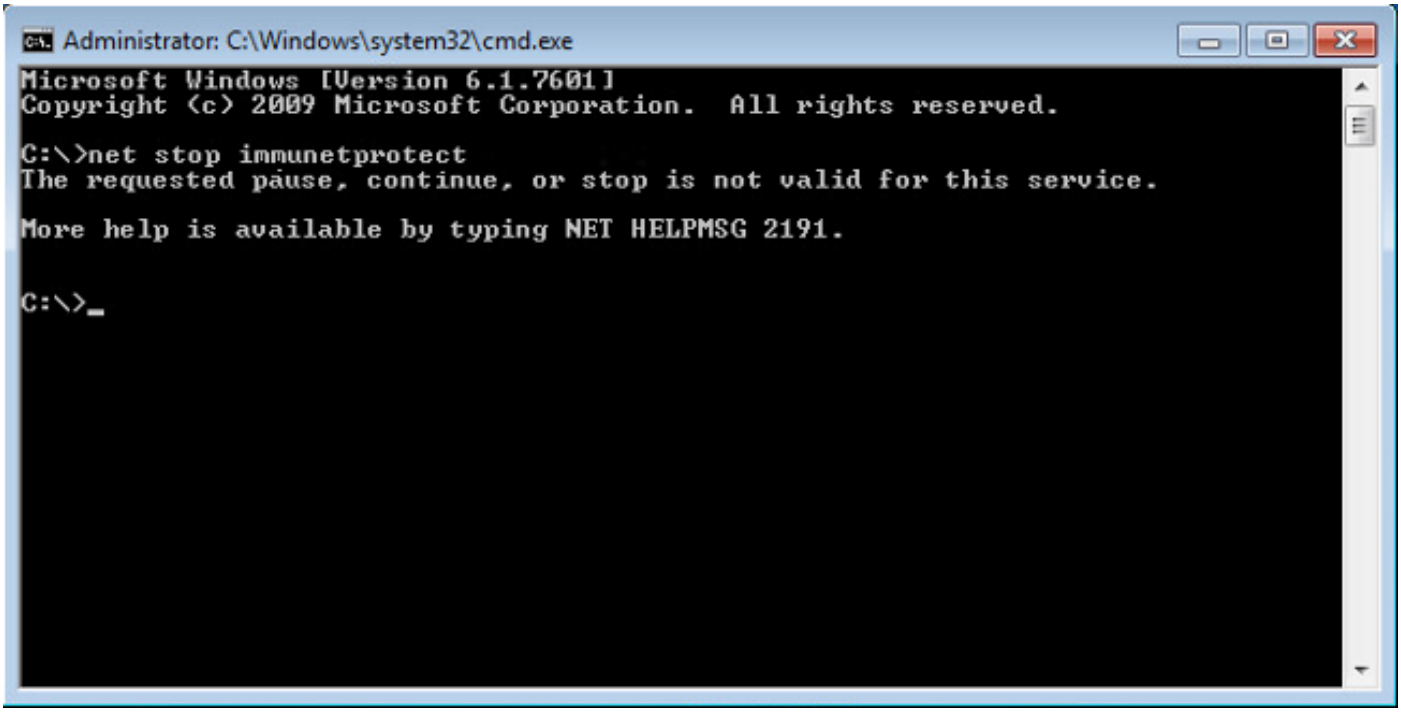
如果啟用了聯結器保護功能，**您將無法使**用**「FireAMP連線**器屬性」**窗**口停止服務。管理服務的按鈕被禁用，如下所示：



使用CLI停止服務

在啟用聯結器保護功能時嘗試停止服務時，會收到如下故障消息：

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



在4.3.0+版上，可以使用「sfc.exe -k password」命令停止sfc.exe服務，其中「password」是在策略中定義的密碼。

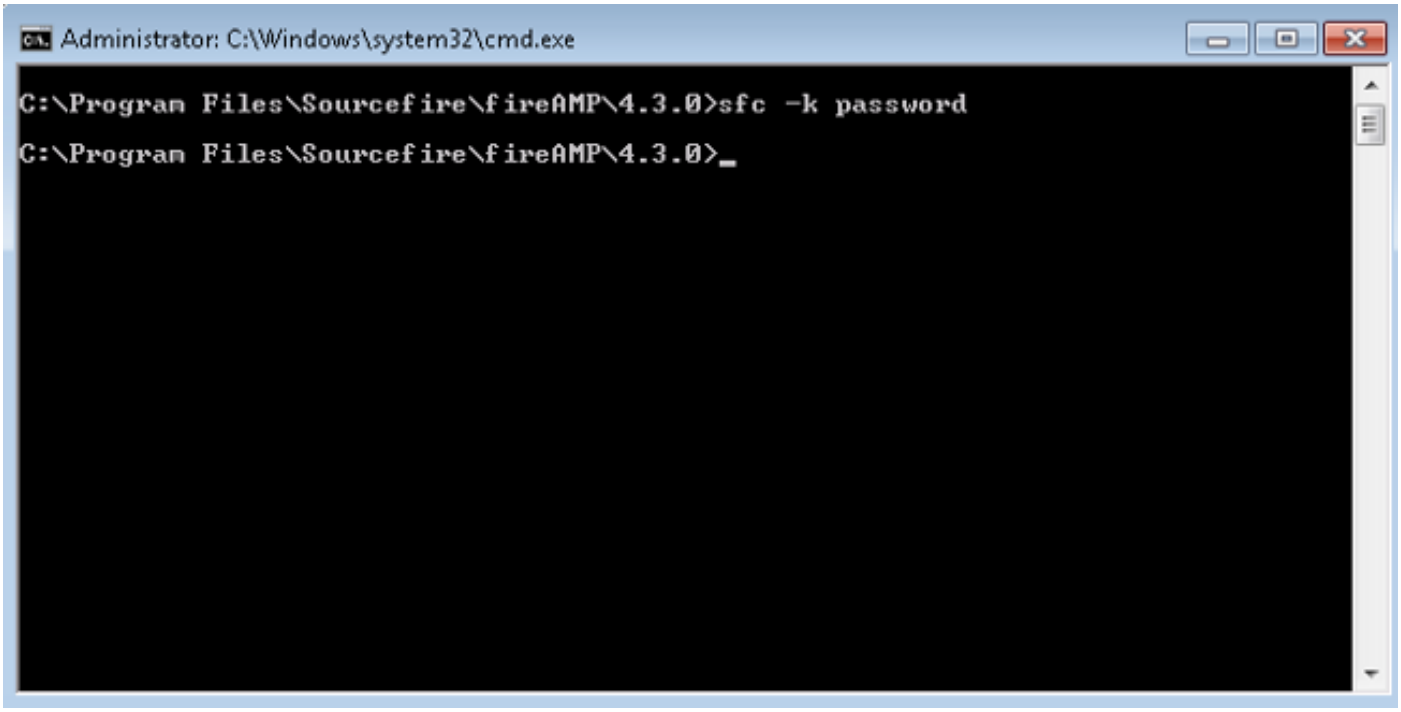
解決方案

使用命令列停止服務

注意 — 此命令僅在4.3.0版及更高版本的FireAMP聯結器上有效。

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

將「password」一詞替換為策略中設定的實際密碼。



使用使用者介面停止服務

可以從使用者介面停止受密碼保護的服務。