コネクタ保護のために FireAMP コネクタ サービスを停止できない

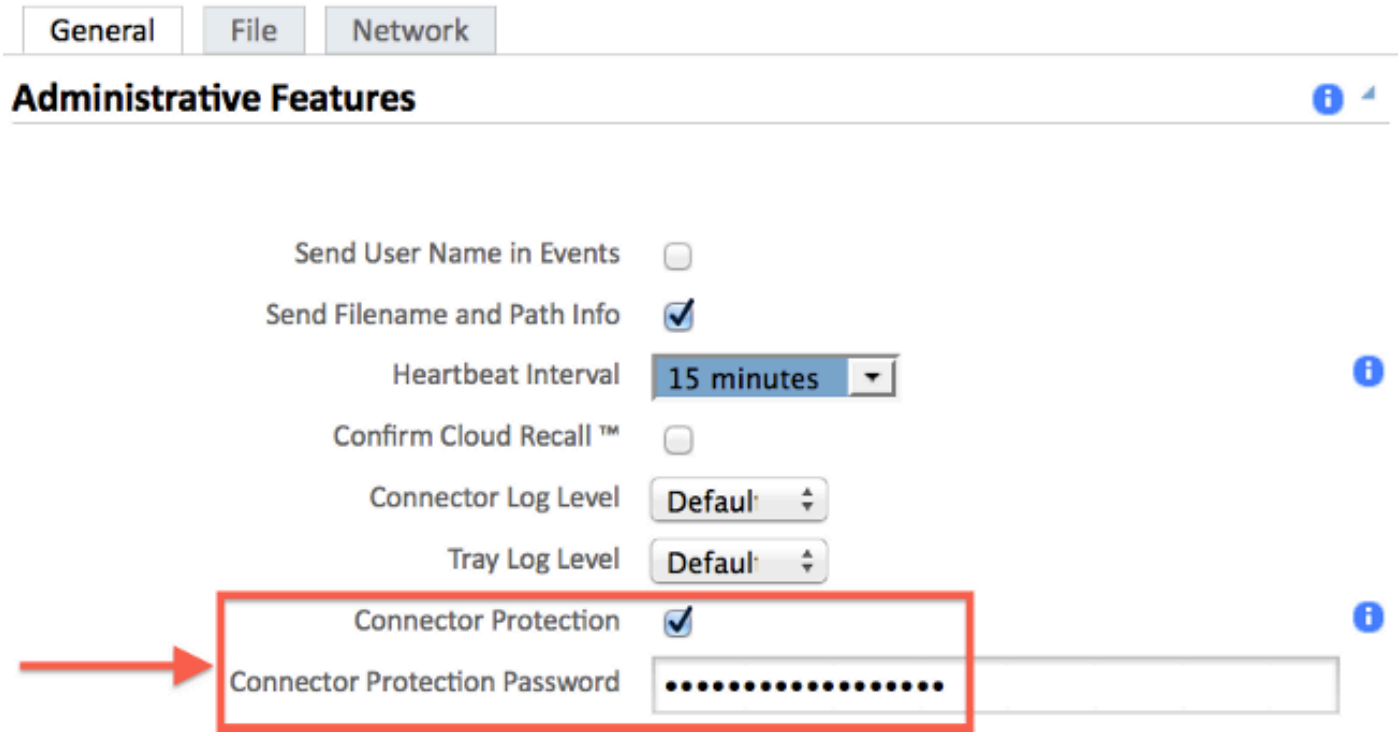
内容

概要

FireAMP コネクタには Connector Protection と呼ばれる機能があります。このオプションにより、FireAMP コネクタ サービスをパスワードで保護し、このサービスが停止またはアンインストールされることがないようにできます。ただし、トラブルシューティングの手順として FireAMP コネクタ サービスの停止またはアンインストールを行うことがあるため、これはトラブルシューティング プロセスに影響する可能性があります。このドキュメントでは、パスワード保護されている FireAMP のアンインストール方法について説明します。

Connector Protection の設定

[Connector Protection] **オプションを有効にするには、ポリシー**を編集します。[General] **タブで [Administrative Features]** を展開します。



自己保護ドライバ

Connector Protection 機能は、自己保護ドライバを使用して FireAMP のディレクトリを保護します。自己保護ドライバは次のタスクを実行します。

1. FireAMPが使用するレジストリキーの削除と変更を防止します。
2. アプリケーションがインストールディレクトリ内のファイルを書き込んだり削除したりするのを防ぎます。デフォルトのインストール ディレクトリは次のとおりです。

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

を選択します。 FireAMPドライバがアンロードされたり、上書きされたりしないように保護します。
4. FireAMPアプリケーション、iptray.exeおよびagent.exeを、Windows Task Managerから「End Processed」から保護します。

FireAMP コネクタ サービスの停止

停止の理由

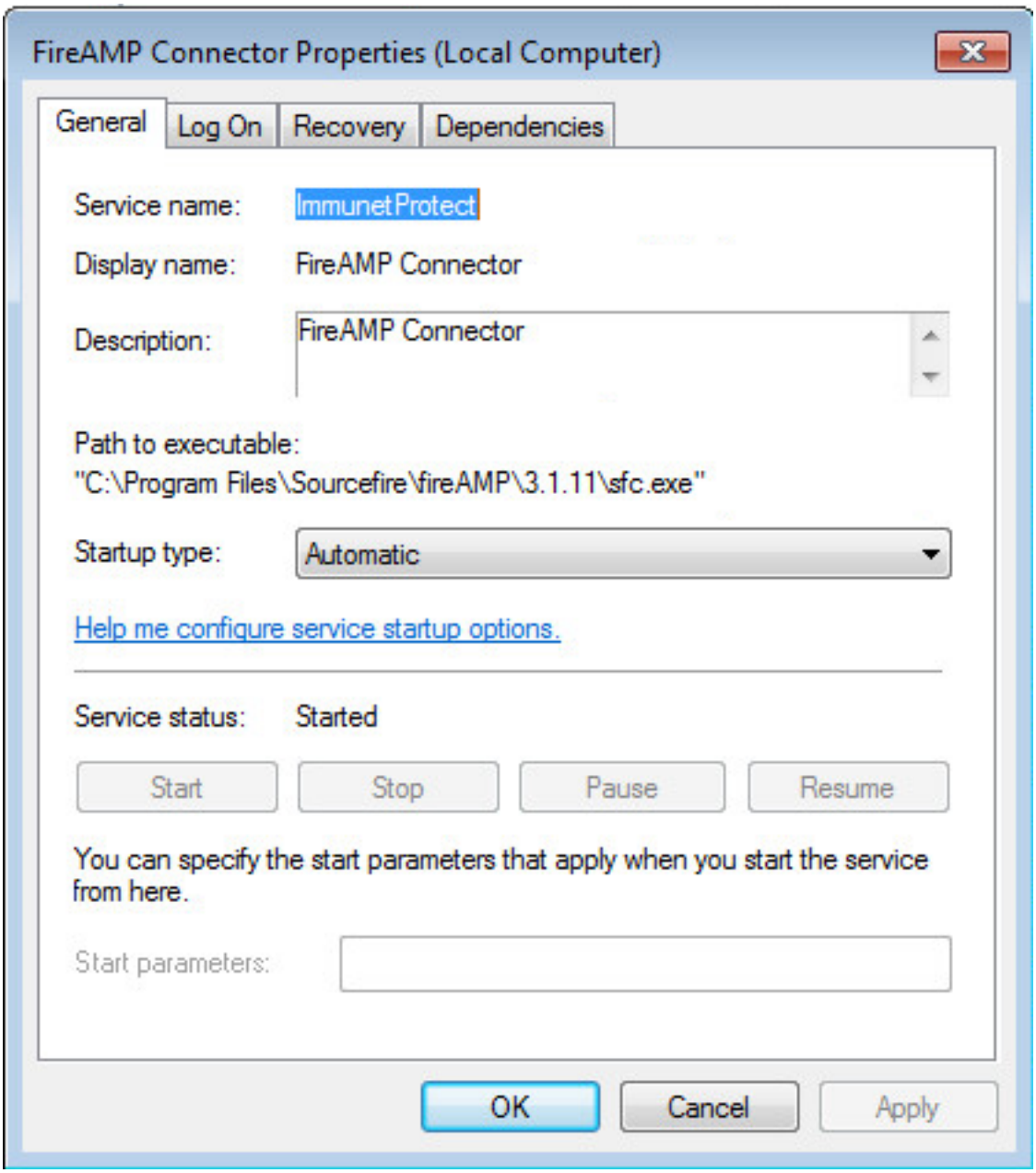
FireAMP コネクタ サービスを停止するか、または FireAMP をアンインストールするのは、次のような状況です。

1. 破損したデータベース ファイルまたは古いログ ファイルを削除するためにサービスを停止する。
2. インストールでエラーや破損が発生したか、またはインストールが不完全であるため、FireAMP をアンインストールする。

3. 接続の問題を診断するため、policy.xml ファイルを置換する。

コネクタ プロパティを使用したサービスの停止

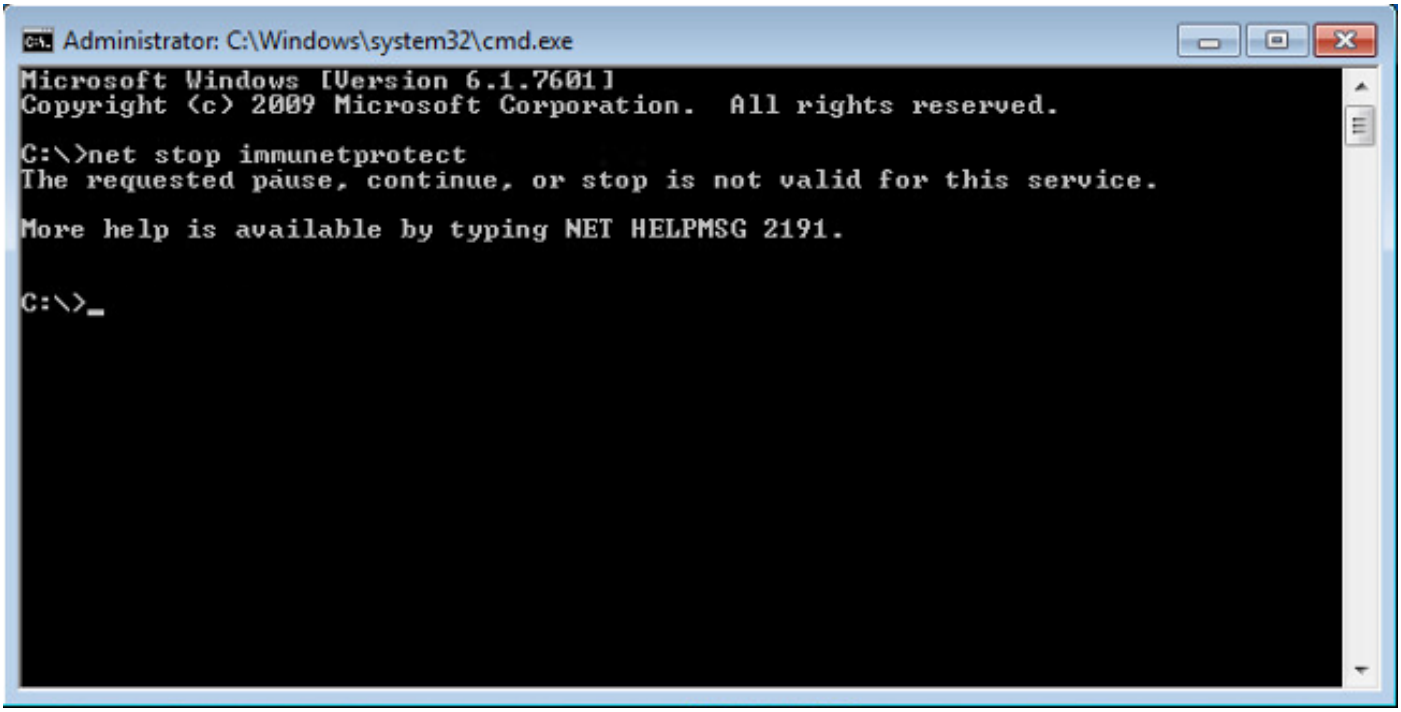
[Connector Protection] **機能が有効な場合に、[FireAMP Connector Properties] ウィンドウを使用してサービスを停止することはできません。**サービス管理のためのボタンは、次に示すように無効になっています。



CLI を使用したサービスの停止

Connector Protection 機能が有効な場合にサービスを停止しようとすると、次のようなエラー メッセージが表示されます。

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



バージョン 4.3.0+ では、「sfc.exe -k password」コマンドを使用して sfc.exe サービスを停止できます。この「password」は、ポリシーで定義されているパスワードです。

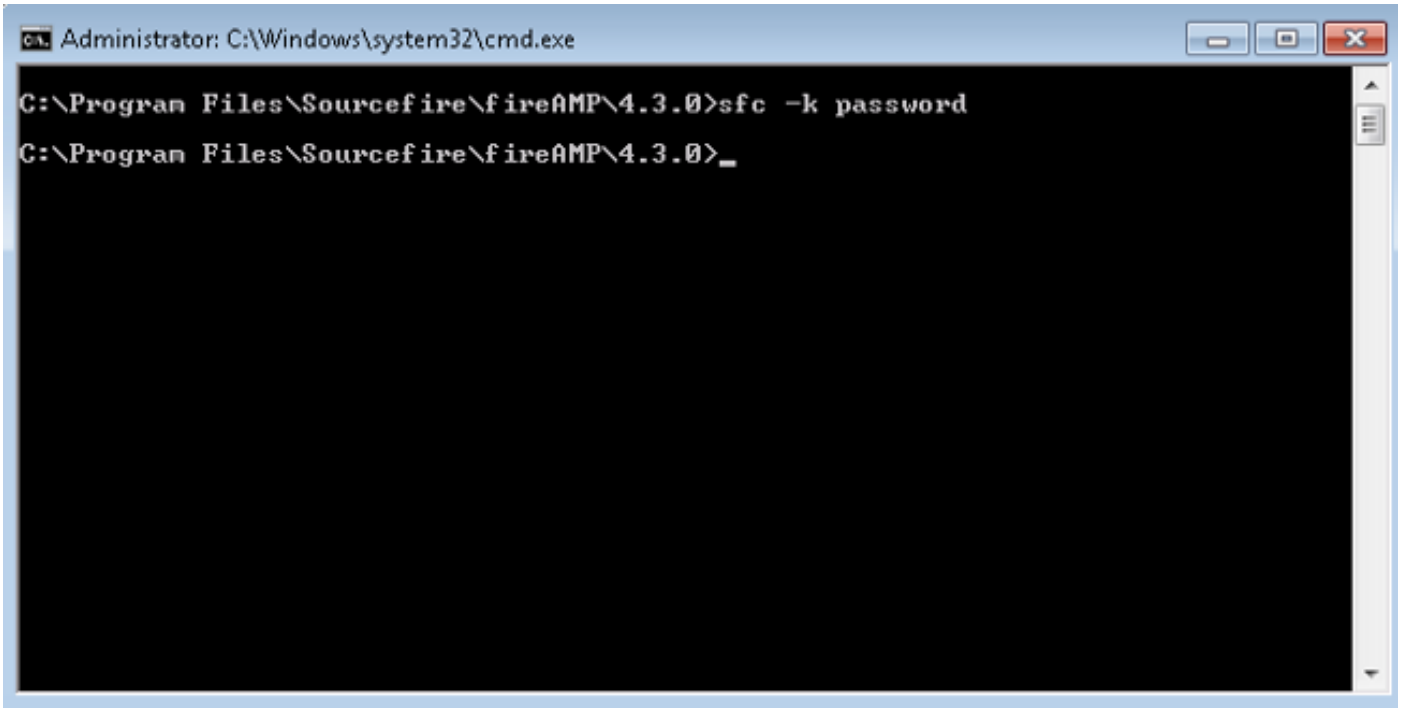
解決方法

コマンド ラインを使用したサービスの停止

注：このコマンドは FireAMP Connector バージョン 4.3.0 以降でのみ機能します。

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

「password」を、ポリシーで設定されている実際のパスワードに置き換えます。



ユーザ インターフェイスを使用したサービスの停止

ユーザ インターフェイスから、パスワード保護されているサービスを停止できます。