由于连接器保护，FireAMP连接器服务无法停止

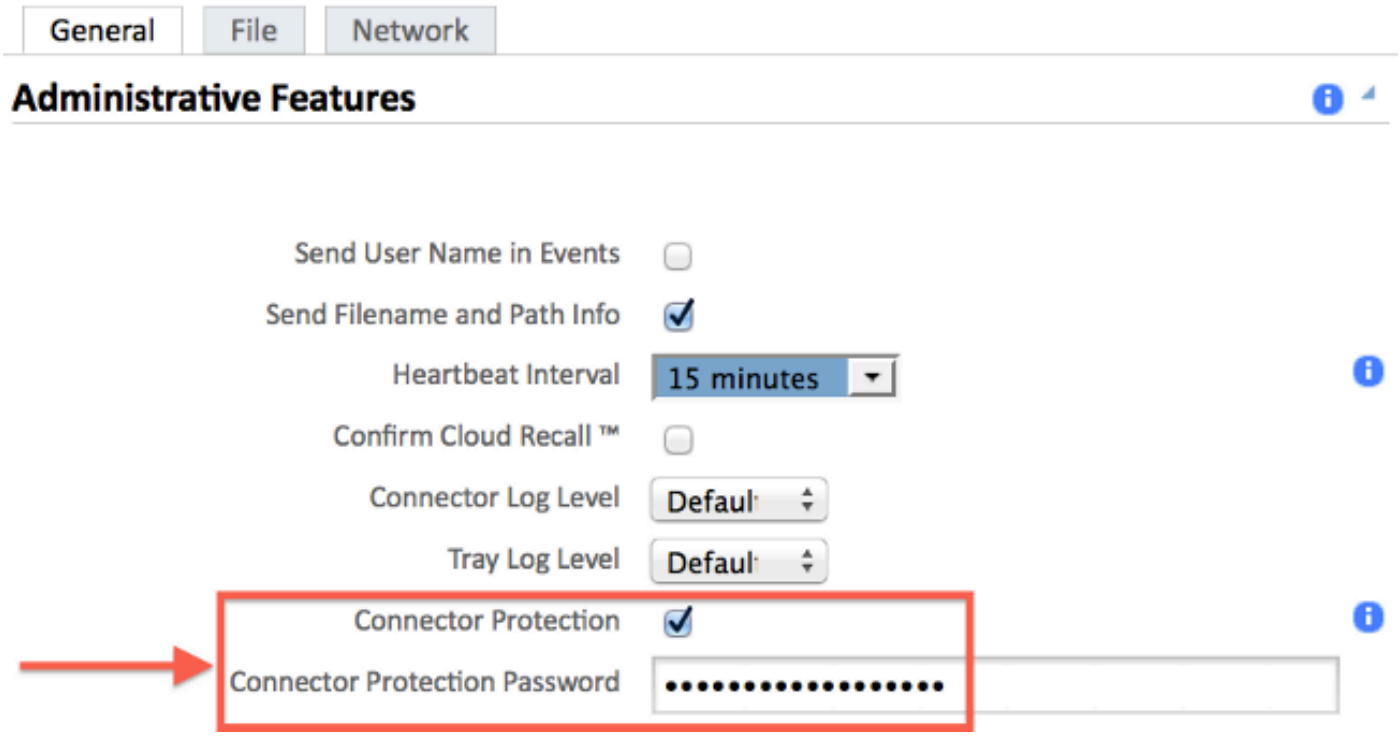
目录

简介

FireAMP连接器具有称为连接器保**护的功能**。此选项允许您对FireAMP连接器服务进行密码保护，并防止其停止或卸载。但是，由于停止FireAMP连接器服务或卸载服务可作为故障排除步骤发挥作用，因此，它可能会影响故障排除过程。本文档介绍如何在FireAMP受密码保护时卸载它。

连接器保护配置

要启用连接器保**护选**项，请编辑**策略**，转到**常规**选项卡，然后展开**管理功能**。



自保护驱动程序

连接器保护功能利用自保护驱动程序来保护FireAMP的目录。自保护驱动程序执行以下任务：

1. 保护FireAMP使用的注册表项不被删除和修改。
2. 防止应用程序在安装目录中写入或删除文件。默认安装目录为：

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

3. 防止卸载或覆盖FireAMP驱动程序。
4. 通过Windows任务管理器保护FireAMP应用程序iptray.exe和agent.exe不被“最终处理”。

停止FireAMP连接器服务

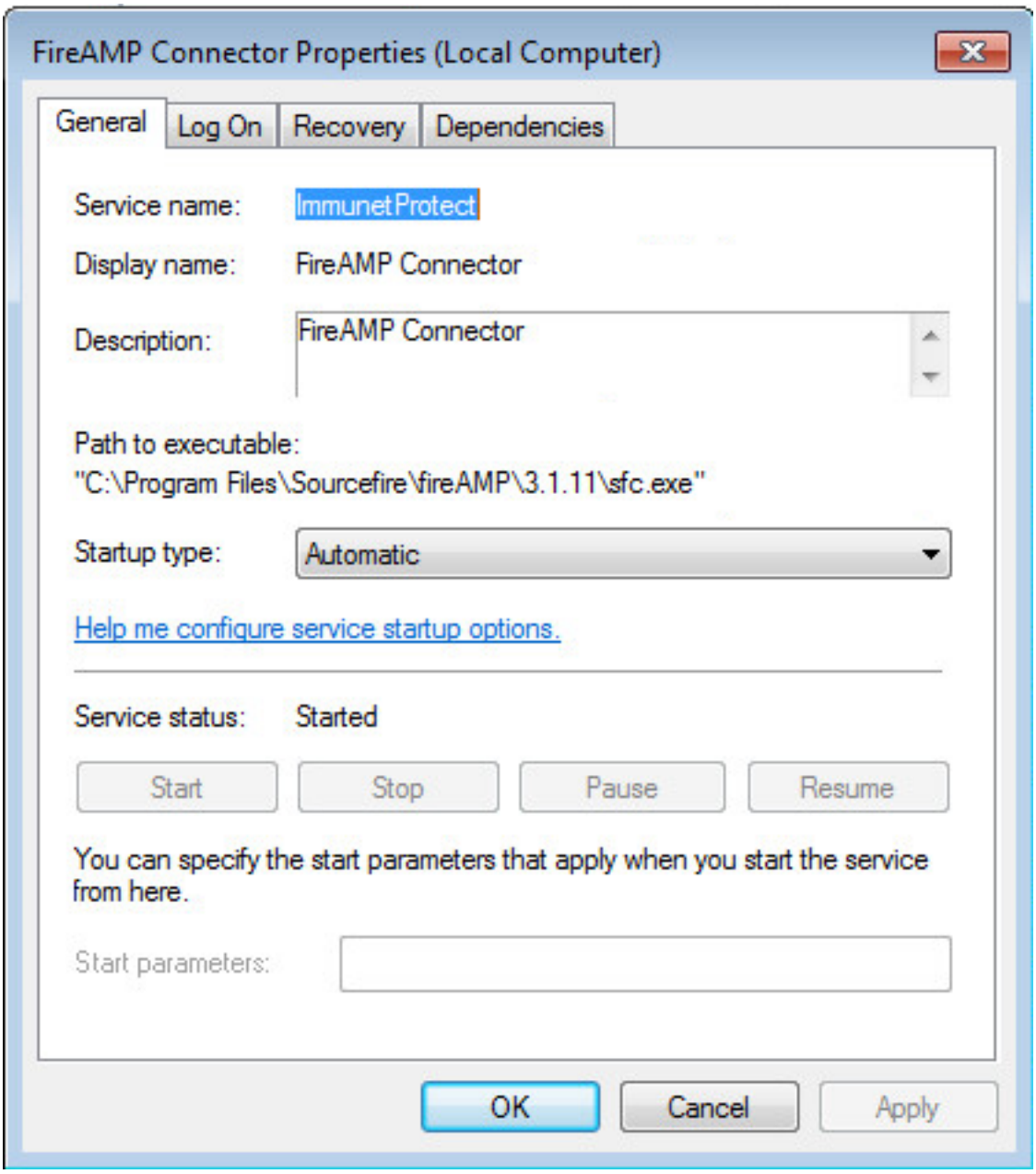
停止的原因

您可能希望停止FireAMP连接器服务或卸载FireAMP的一些场景是：

1. 停止服务以删除损坏的数据库文件或旧日志文件。
2. 由于错误、损坏或安装不完整，请卸载FireAMP。
3. 替换policy.xml文件以诊断连接问题。

使用连接器属性停止服务

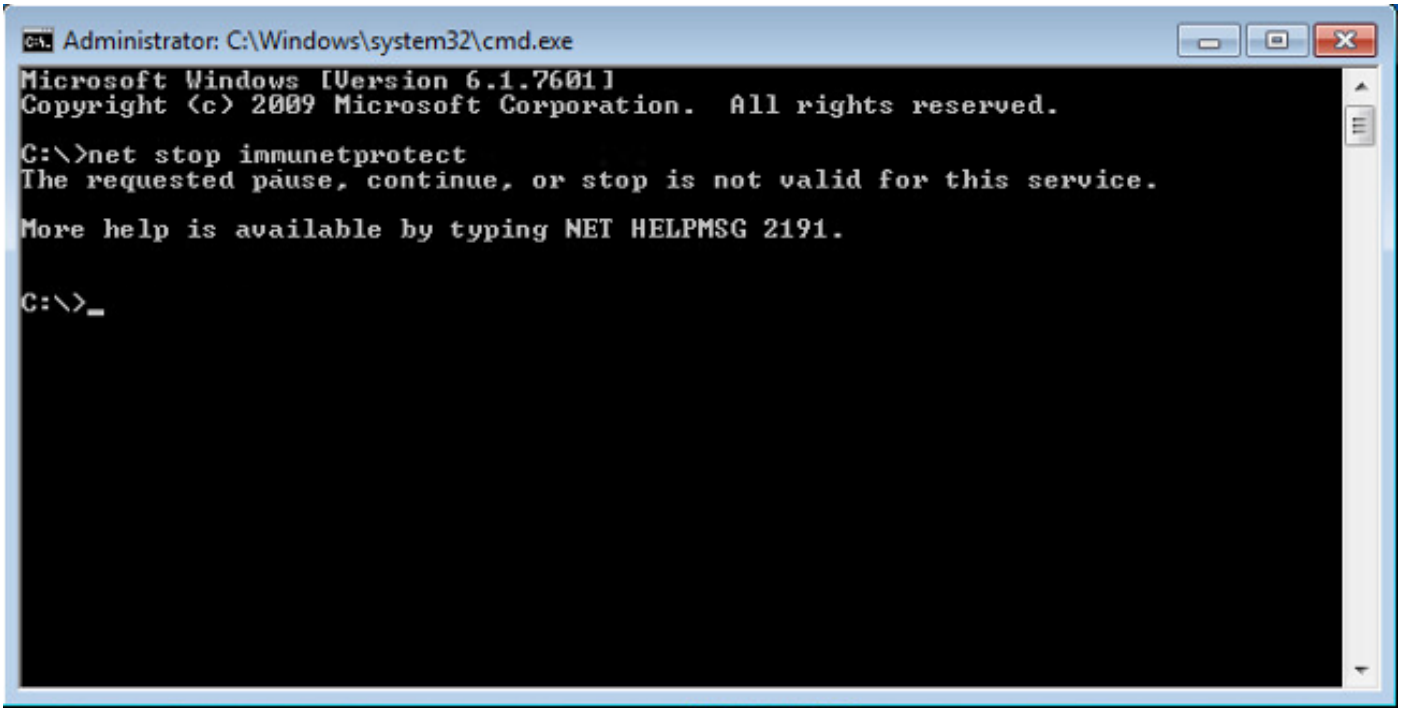
如果启用了连接器保护功能，则无**法使用FireAMP**连接器属**性窗**口停止服务。管理服务的按钮禁用如下：



使用CLI停止服务

当您尝试在启用连接器保护功能时停止服务时，您会收到如下所示的失败消息：

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



在版本4.3.0+上，使用命令“sfc.exe -k password”可停止sfc.exe服务，其中“password”是策略中定义的密码。

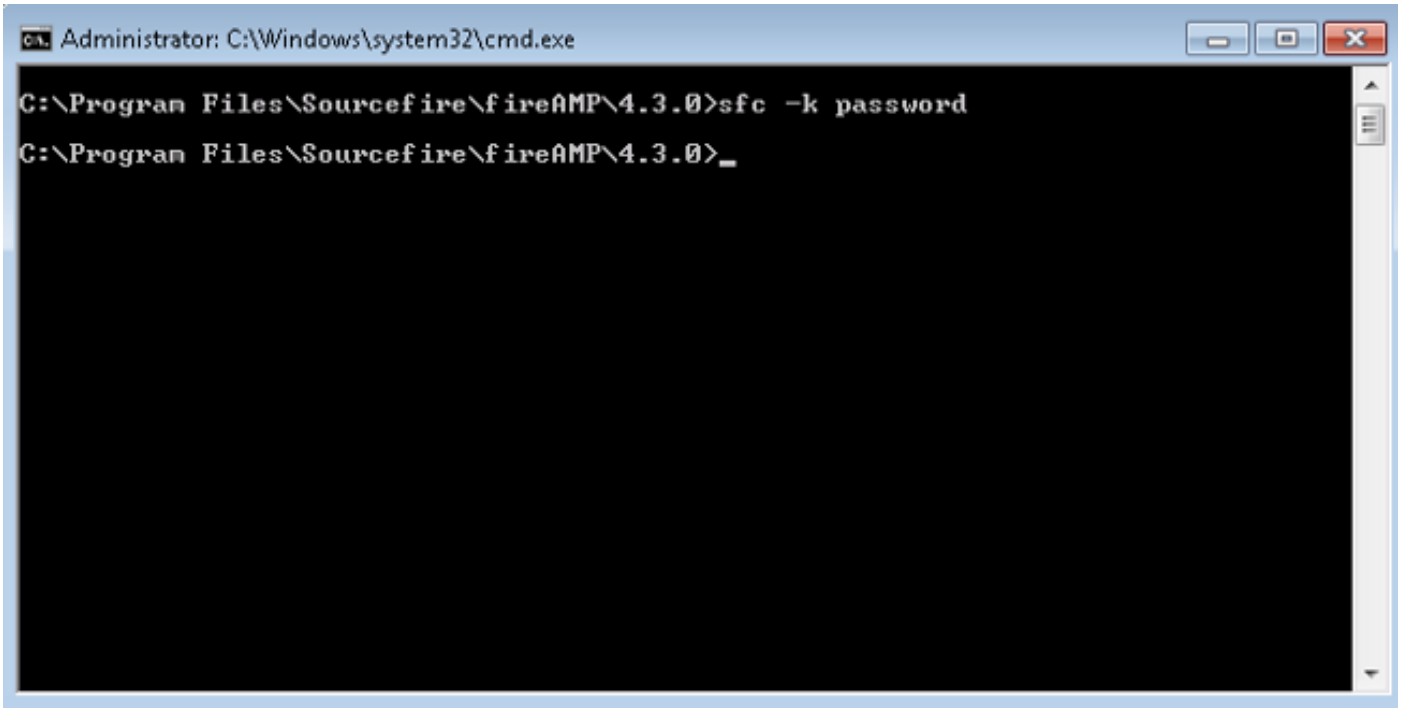
解决方案

使用命令行停止服务

注意 — 此命令仅在FireAMP连接器的4.3.0版及更高版本上有效。

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

将“password”一词替换为策略中设置的实际密码。



使用用户界面停止服务

您可以从用户界面停止受密码保护的服务。