FireAMP Connector Service Fails to Stop due to Connector Protection

TAC **Document ID: 118701**

Contributed by Nazmul Rajib and Alexander Dipasquale, Cisco TAC Engineers.
Jan 28, 2016

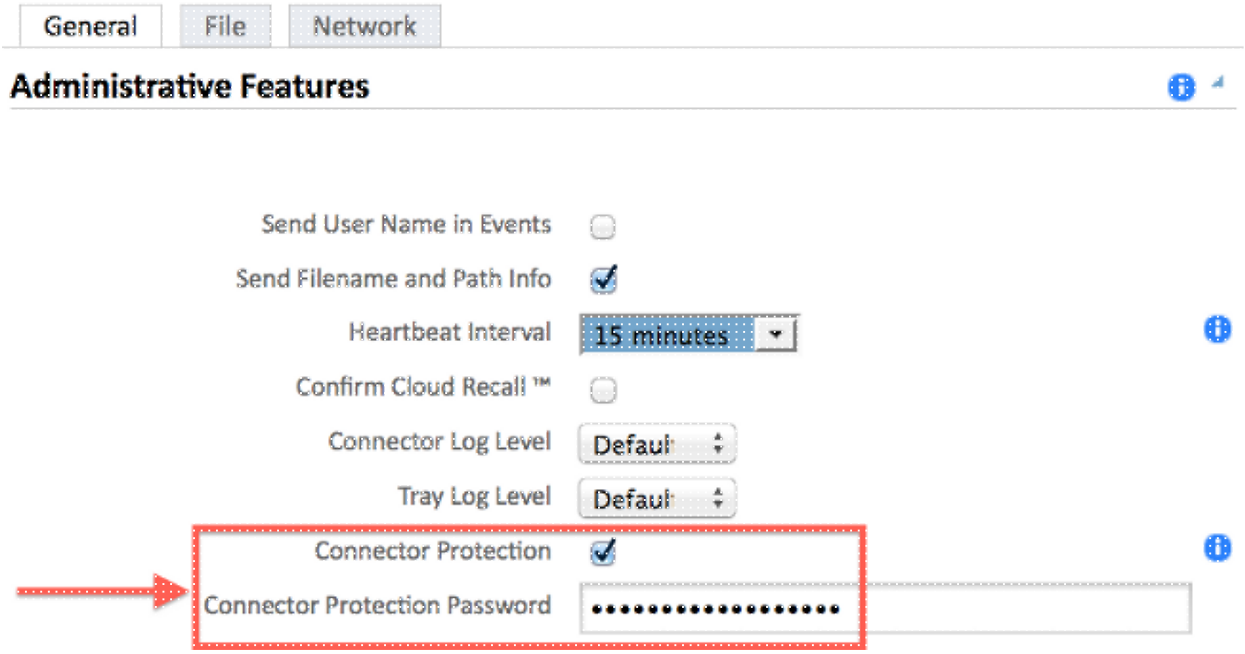
Contents

Introduction

The FireAMP Connector has a feature called **Connector Protection**. This option allows you to password protect the FireAMP Connector service and prevent it from being stopped or uninstalled. However, it may impact troubleshooting process due to the fact that stopping the FireAMP connector service or uninstalling it can come in to play as a troubleshooting step. This document describes how to uninstall FireAMP when it is password protected.

Configuration of Connector Protection

In order to enable the **Connector Protection** option, edit your **Policy**, go to the **General** tab, and expand **Administrative Features**.



Self Protect Driver

Connector Protection feature utilizes a self-protect driver to protect the directories for FireAMP. A self-protect driver performs the following tasks:

1. Protect registry keys that FireAMP uses from being deleted and modified.
2. Protect applications from writing or deleting files in the installation directory. The default installation directory is:

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

3. Protect the FireAMP drivers from being unloaded or overwritten.
4. Protect FireAMP applications, iptray.exe and agent.exe, from being "End Processed" via Windows Task Manager.

Stopping FireAMP Connector Service

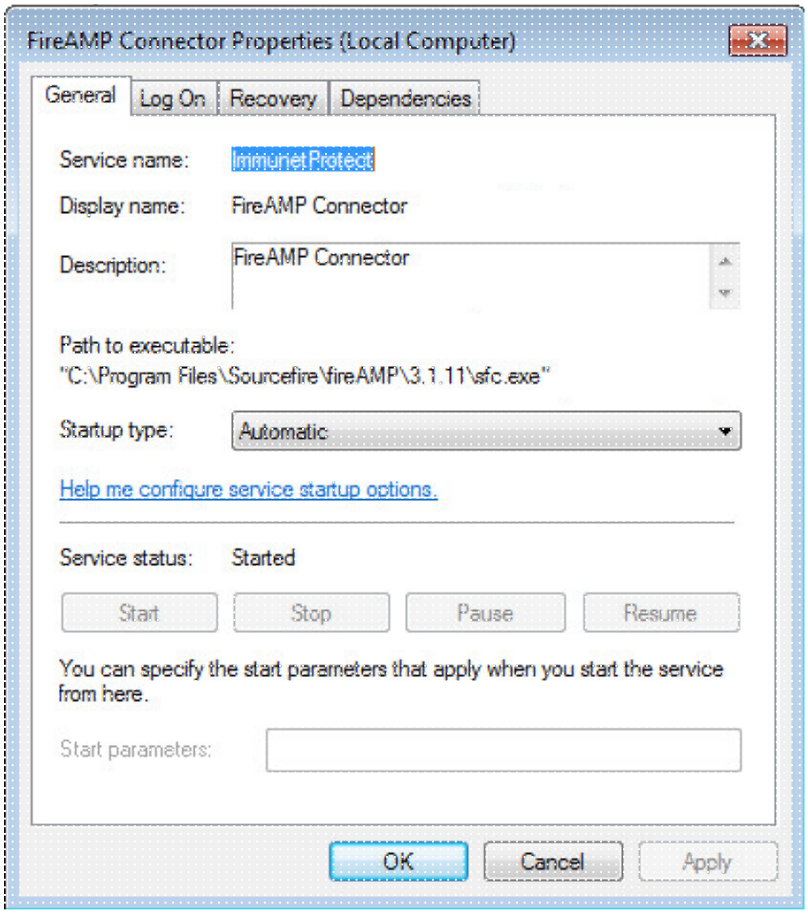
Reasons for a Stop

Some scenarios where you may want to stop the FireAMP connector service or uninstall FireAMP would be:

1. Stop the service in order to remove corrupt database files, or old log files.
2. Uninstall FireAMP due to an error, corrupt, or incomplete installation.
3. Replace the policy.xml file in order to diagnose connectivity issues.

Stop Service Using Connector Properties

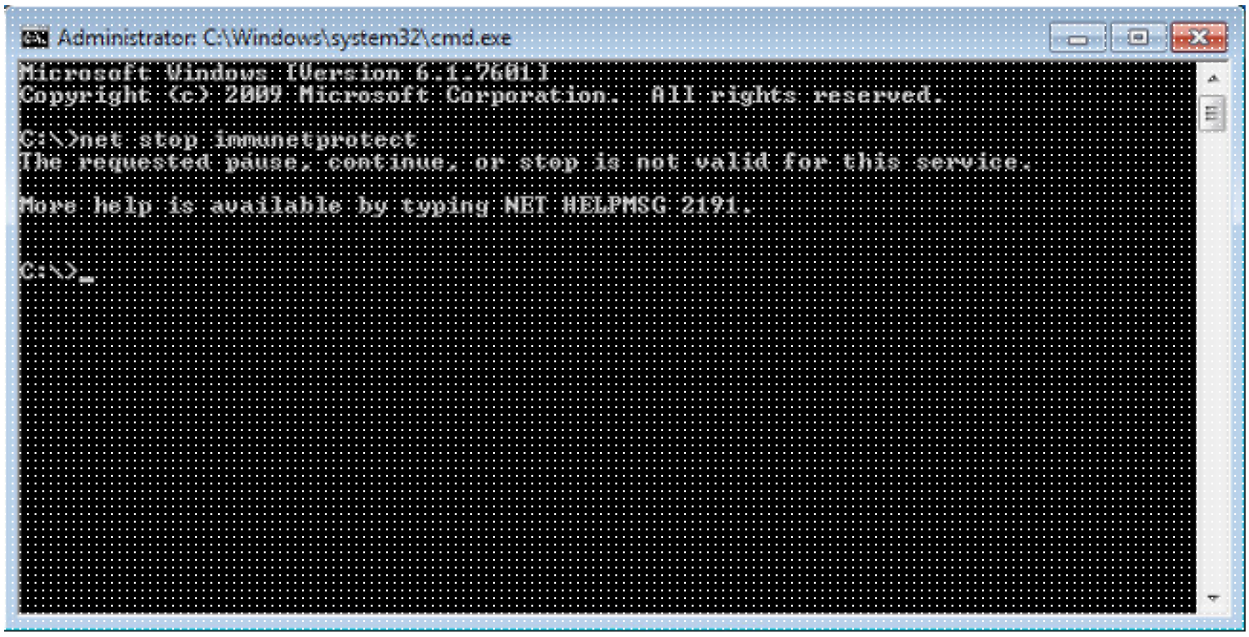
You will not be able to stop service using the **FireAMP Connector Properties** window if the **Connector Protection** feature is enabled. The buttons to manage the service are disabled as below:



Stop Service Using CLI

When you attempt to stop a service while the connector protection feature is enabled, you receive a failure message like below:

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



On version 4.3.0+ the sfc.exe service can be stopped with the command "sfc.exe -k password" where

'password' is the password defined in the policy.

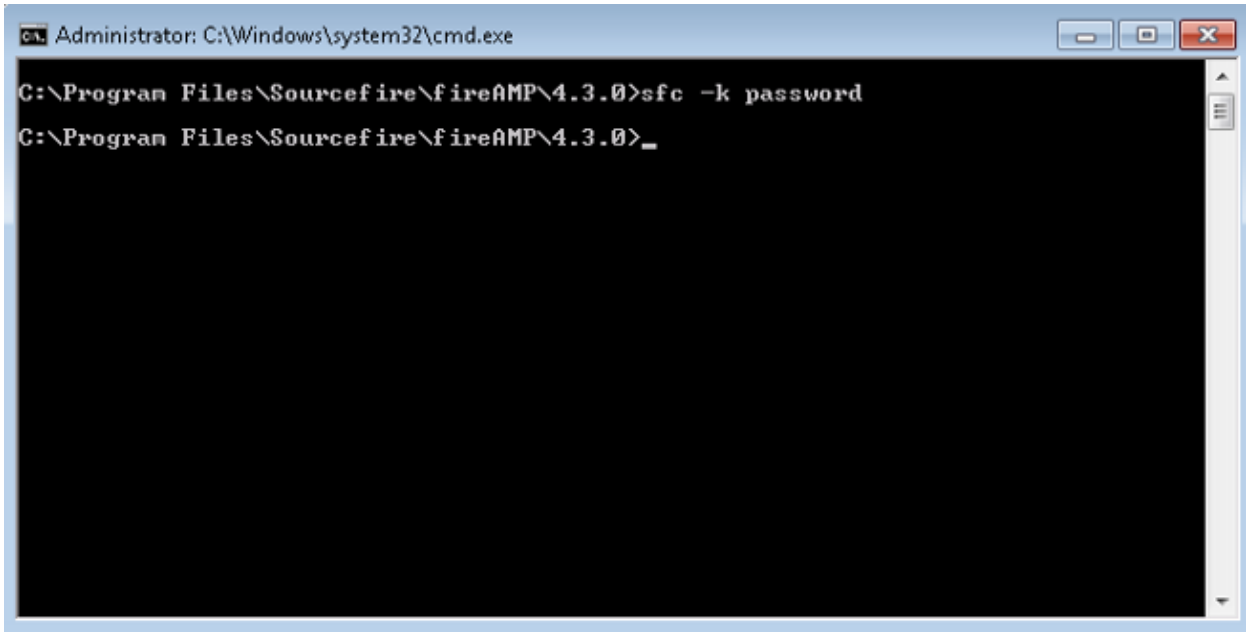
Solution

Stop the service using the Command Line

Note - This command only works on version 4.3.0 and higher of the FireAMP Connector.

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

Replace the word "password" with the actual password set in your policy.



Stop Service using the User Interface

You can stop the password protected service from the user interface.