诊断数据的集从一FireAMP连接器运行的在Windows

目录

简介

本文描述步骤生成从FireAMP连接器的诊断文件。如果遇到一个技术问题用在Microsoft Windows运行的FireAMP连接器，思科技术支持工程师也许要分析日志消息可用在诊断文件。

生成诊断文件

从属在Windows版本，定位对FireAMP连接器支持诊断工具也许不同的。在多数Windows操作系统中，您去Start菜单为了查找FireAMP连接器支持诊断工具。例如：

开始>所有Programs> FireAMP连接器>支持诊断工具。

> **注意**：如果有用户帐户的Run窗口控制，请点击**是**为了允许工具运行。

支持诊断工具在桌面创建在7z格式的一个压缩文件并且保存它。这是诊断文件的文件名的示例在桌面的：

v5.0和及早： `Sourcefire_Support_Tool_YYYY_MM_DD_HH_MM_SS.7z`

v5.1 `CiscoAMP_Support_Tool_YYYY_MM_DD_HH_MM_SS.7z`

或者，您能运行此可执行文件作为管理员：

```
v5.0 and earlier: C:\Program Files\Sourcefire\fireAMP\X.X.X\ipsupporttool.exe
v5.1 and newer: C:\Program Files\Cisco\AMP\X.X.X\ipsupporttool.exe
```

调试模式

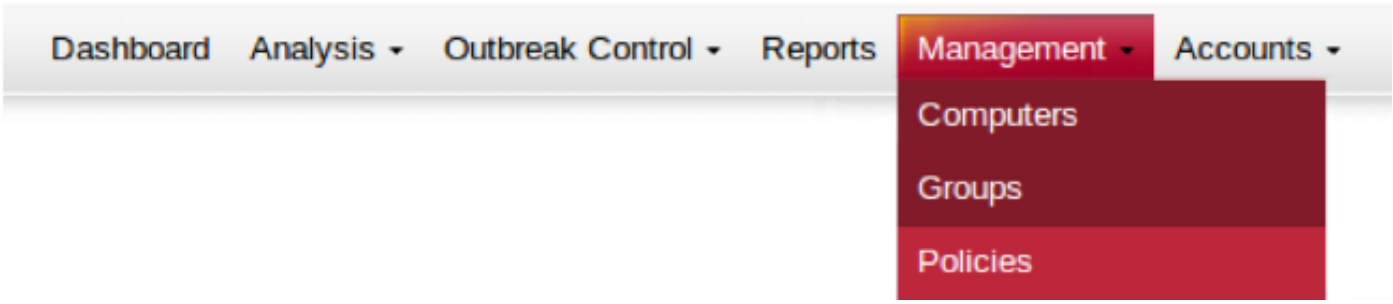
调试模式的能力提升计划在FireAMP连接器的提供另外的冗余给记录日志，准许更多见解到问题用连接器。此部分描述如何启动在FireAMP连接器的调试模式。

> 警告：调试模式，只有当思科技术支持工程师请求此数据，应该启用。启用最长时间的调试模式非常迅速填满磁盘空间并且也许防止支持诊断文件采集**连接器日志**和**盘日志**由于额外的文件大小。

Enable (event)调试模式

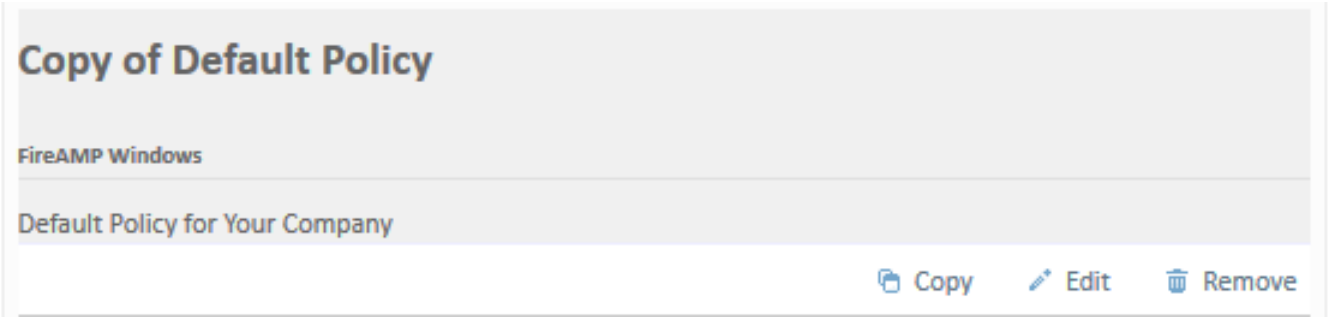
步骤 1：登录FireAMP控制台。

步骤 2：选择**Management>策略**。

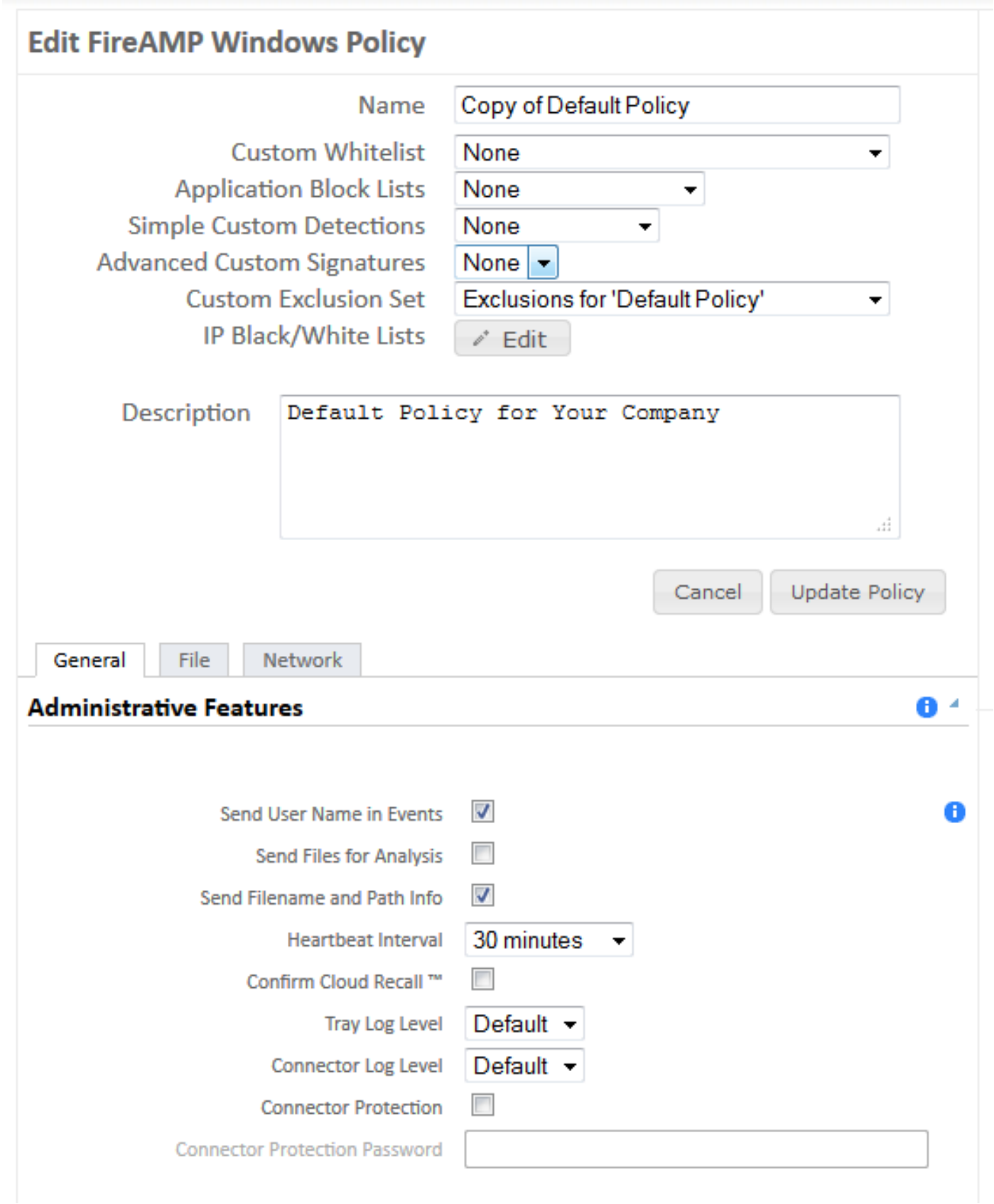


步骤 3：找出应用到终端设备或计算机的策略并且点击**“Copy”。**

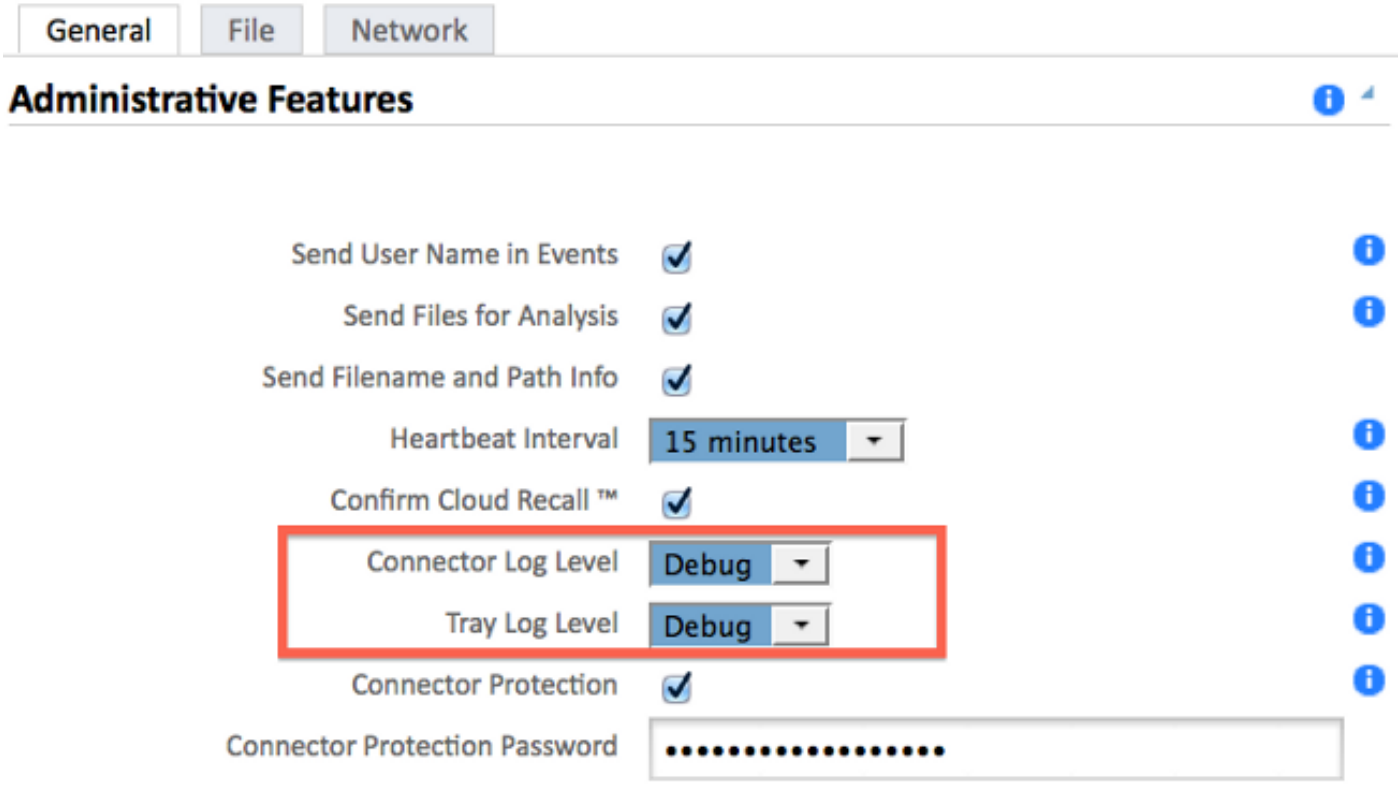
步骤 4：在您点击“Copy”后，与复制的策略的FireAMP控制台更新。



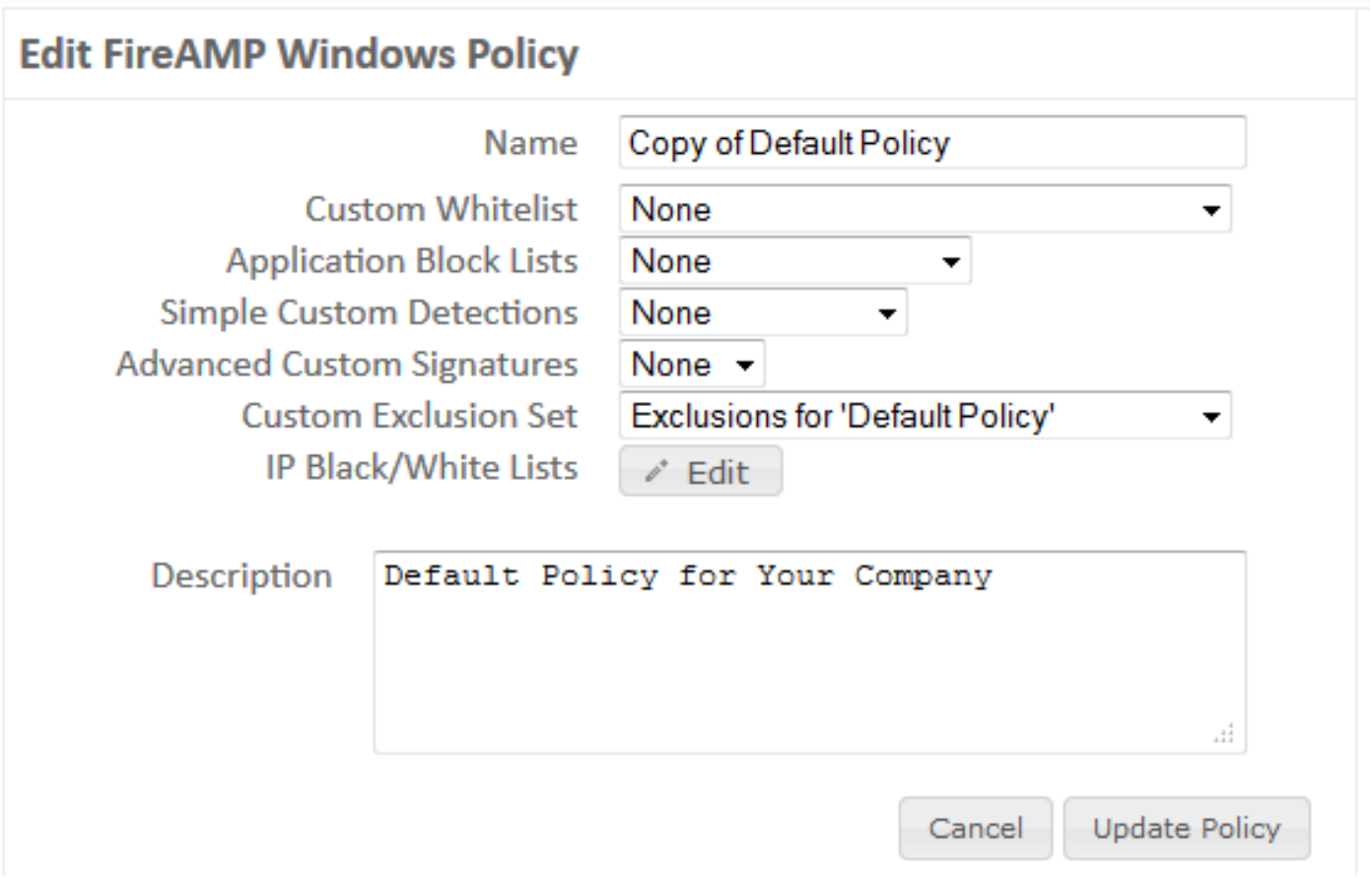
步骤5:Click**编辑**然后单击**管理功能**。



步骤 6：对于**盘日志级别**和**连接器日志级别**，请从下拉列表选择**调试**。



步骤 7：点击**更新策略**为了保存更改。



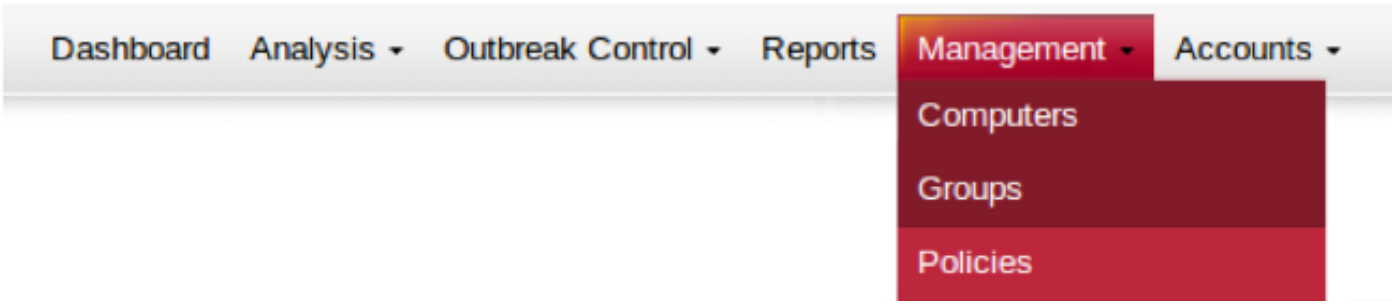
步骤 8:在您更新策略后，您在您要生成调试信息的终端设备需要应用此。

无法启动调试模式

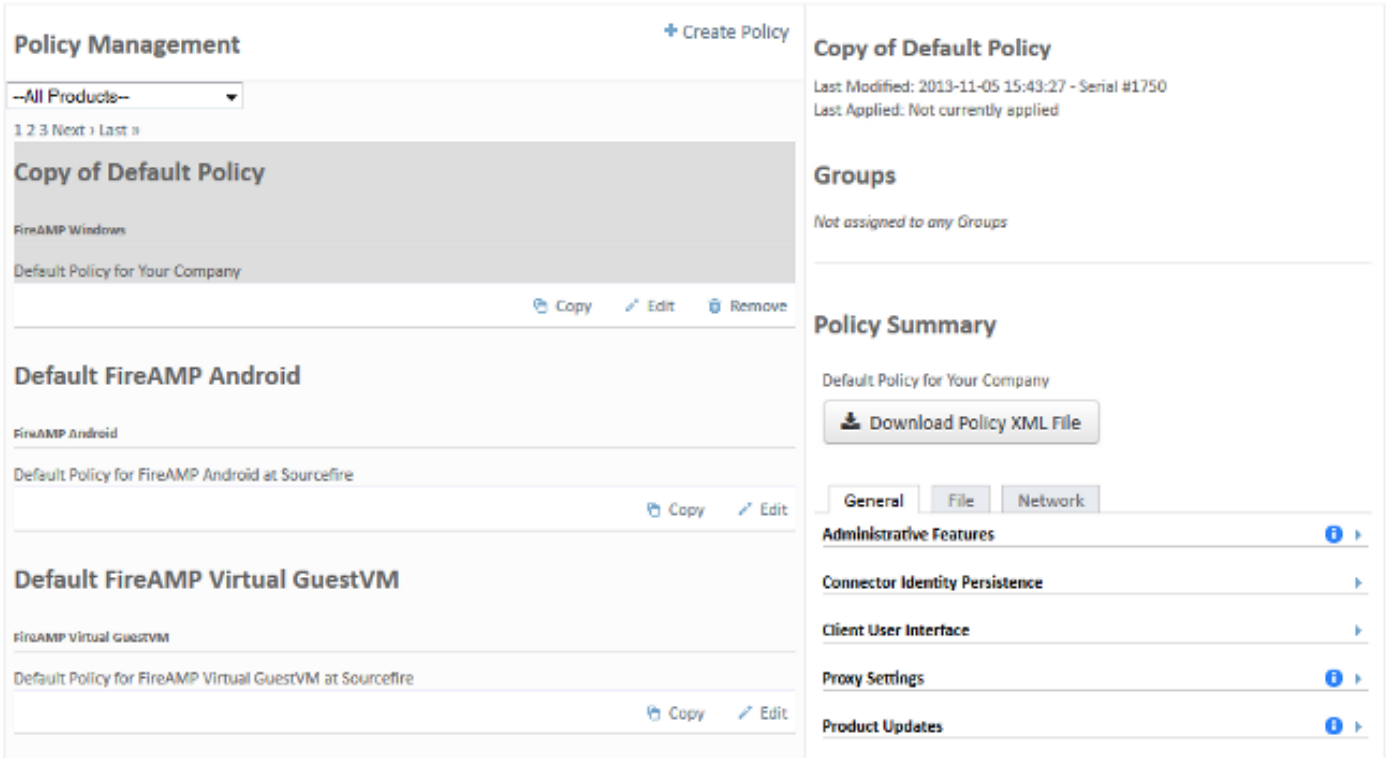
由于连通性问题，如果无法适用于策略FireAMP连接器您无法启动调试模式。在那种情况下，您能

下载policy.xml和配置FireAMP连接器使用您的已修改策略。遵从这些说明FireAMP网云是否无法用FireAMP连接器通信：

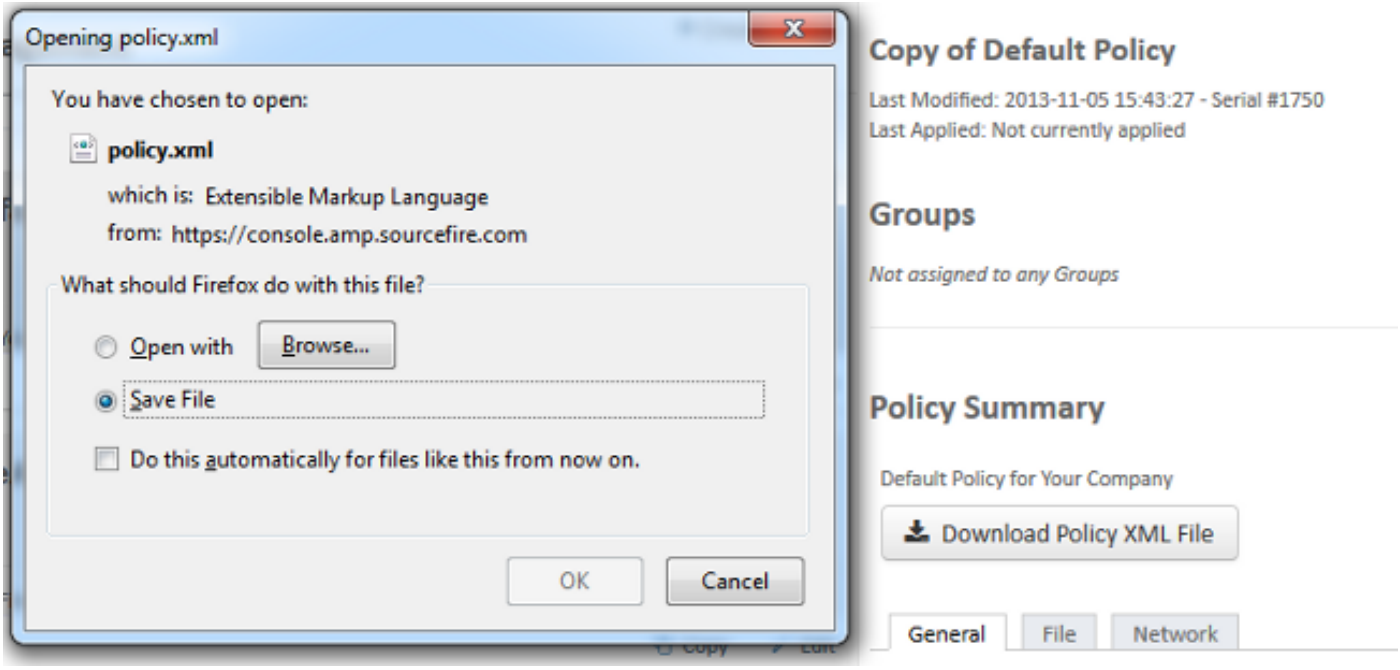
步骤 1：选择**Management>策略**。



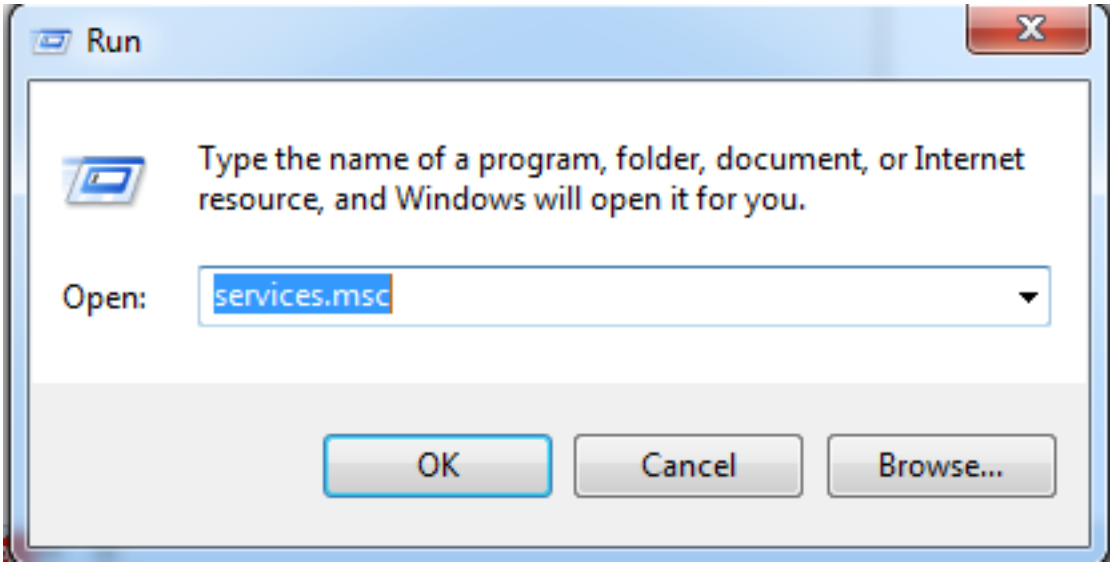
步骤 2：找出复制的策略并且点击命名为了显示**策略摘要**。



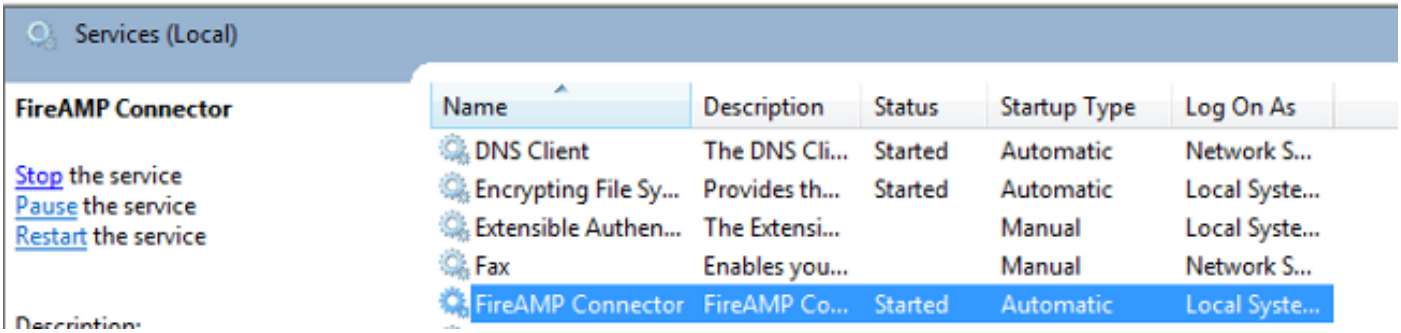
步骤 3：点击**下载策略XML文件**然后保存文件到您的计算机。



步骤 4：打开Start > Run的**services.msc。**



步骤 5：找出**FireAMP连接器**服务并且点击**终止。**



步骤 6：点击**开始>计算机**，然后导航到这些目录之一根据计算机体系结构：

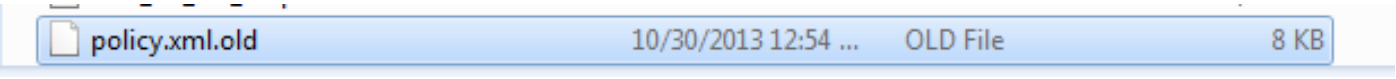
在x86平台中：

```
v5.0 and earlier: C:\Program Files (x86)\Sourcefire\fireAMP
v5.1 and newer: C:\Program Files (x86)\Cisco\AMP
```

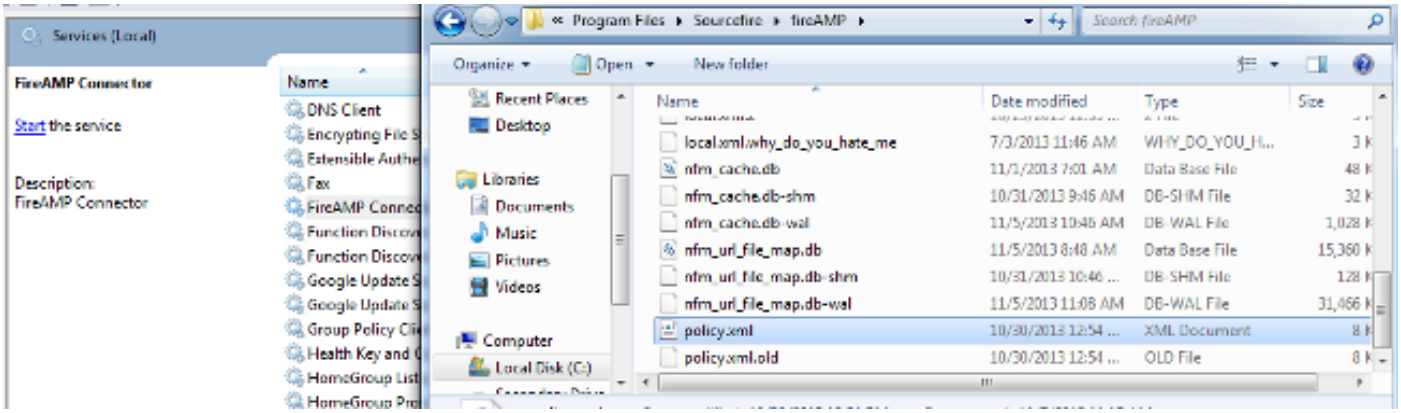
在x64平台中：

```
v5.0 and earlier: C:\Program Files\Sourcefire\fireAMP
v5.1 and newer: C:\Program Files\Cisco\AMP
```

步骤 7：寻找文件`policy.xml`重命名文件对policy.xml.old。



步骤 8:搬入下载的`policy.xml`目录然后单击**在**Services窗口的Startthe**服务**。FireAMP连接器当前是调试模式和日志其他诊断数据。



为了禁用调试模式，请执行步骤5至步骤8，取消对`policy.xml.old`更改FireAMP连接器。