制作镜像或克隆一台计算机用安装的FireAMP连接器

目录

简介

作为系统管理员，您可以要生成您的磁盘镜像或克隆您的硬盘驱动器，并且复制它在其他物理或虚拟系统上。它允许您节约时间和资源。如果您的组织的用户运行有些软件，您在“主图象”可以要包括它，因此每个被克隆的系统有该软件的复制。某个软件例如FireAMP要求独特识别的系统。本文描述进程防止多台计算机尝试使用同一个全局唯一标识符(GUID)，可以防止重复的计算机对象出现在FireAMP网云控制板。它允许FireAMP在一个被克隆的系统上正常运行。

克隆计算机用安装的FireAMP连接器

如果要生成磁盘的镜像或克隆硬盘驱动器，有两接近您能采取：

- 手工方法
- 标识同步

手工方法

您能手工生成“主图象”您的计算机用安装的FireAMP连接器。有两个主要步骤对此进程：

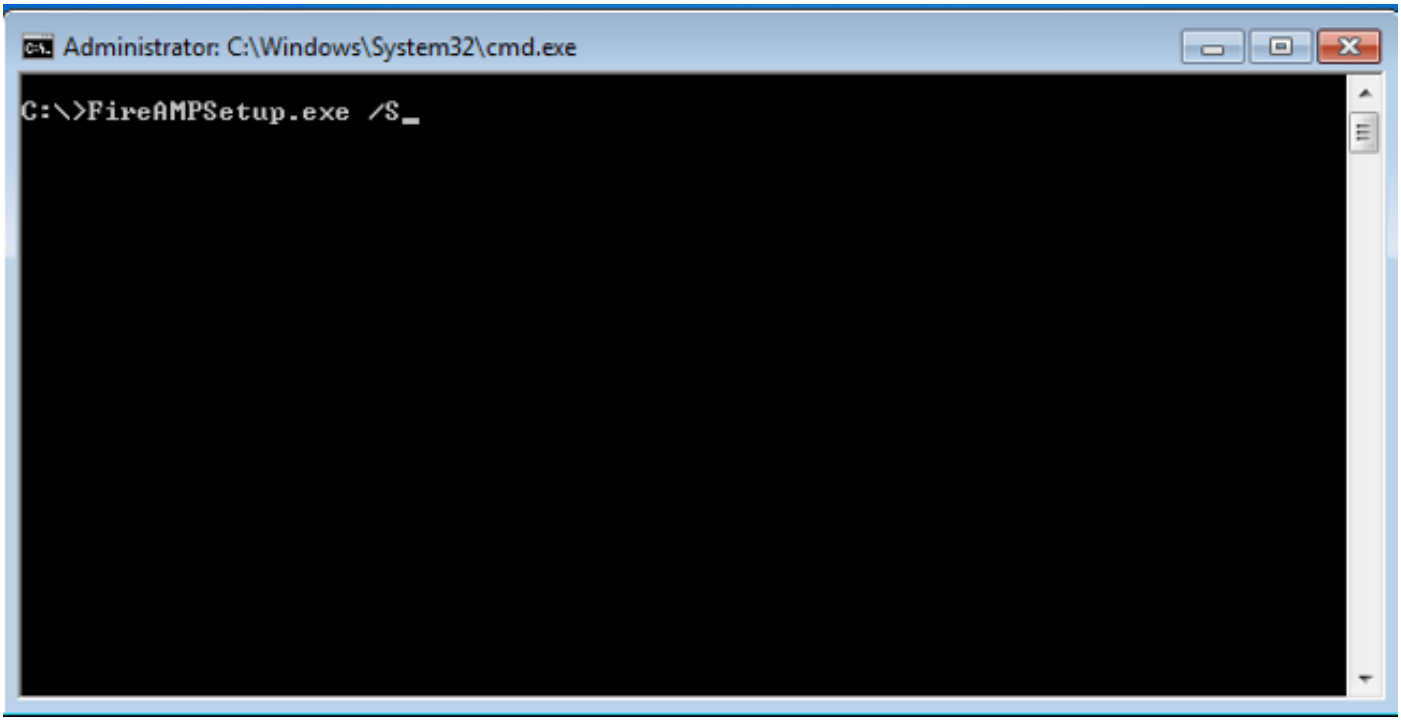
- 装配前准备工作
- 安装后

装配前准备工作

执行以下步骤准备制作镜像的一台计算机：

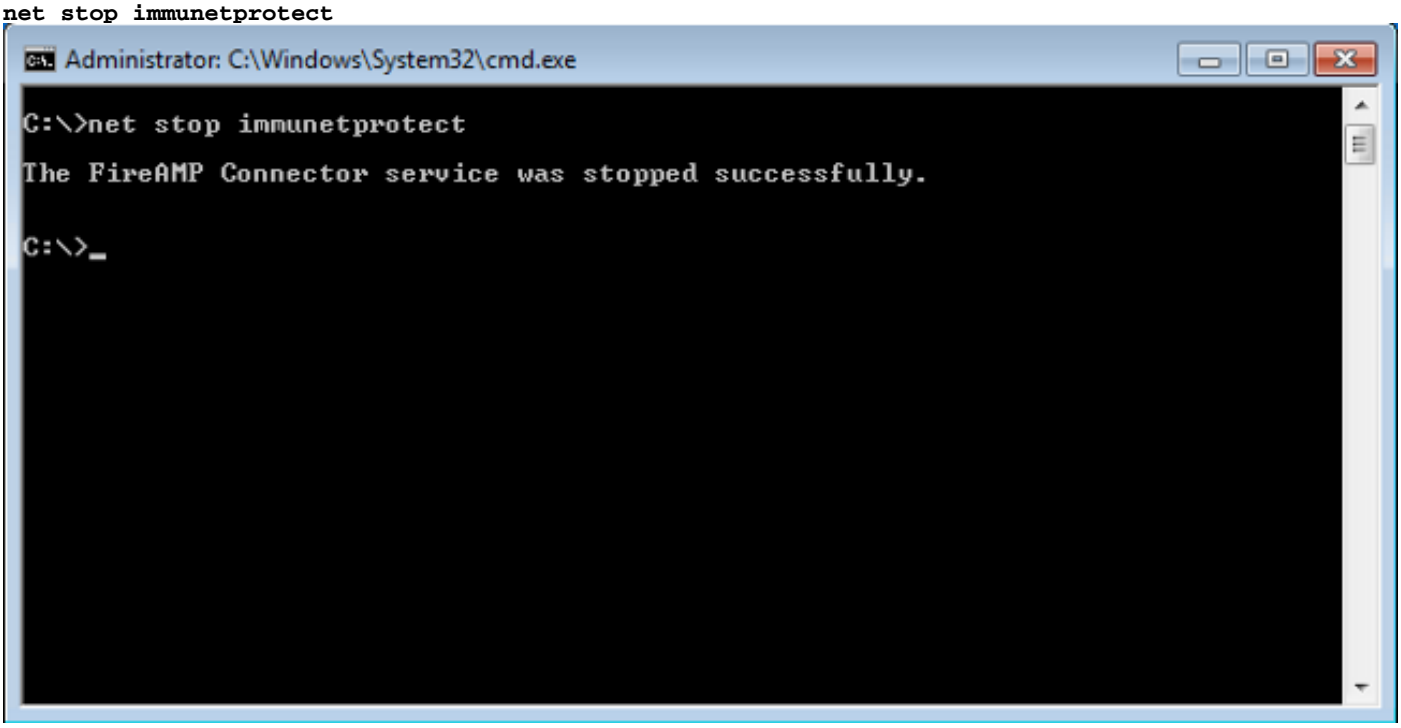
1. 运行FireAMP设置安装程序。

```
FireAMPSetup.exe /S
```



2. 打开prompt命令作为管理员并且通过运行以下命令终止FireAMP连接器：

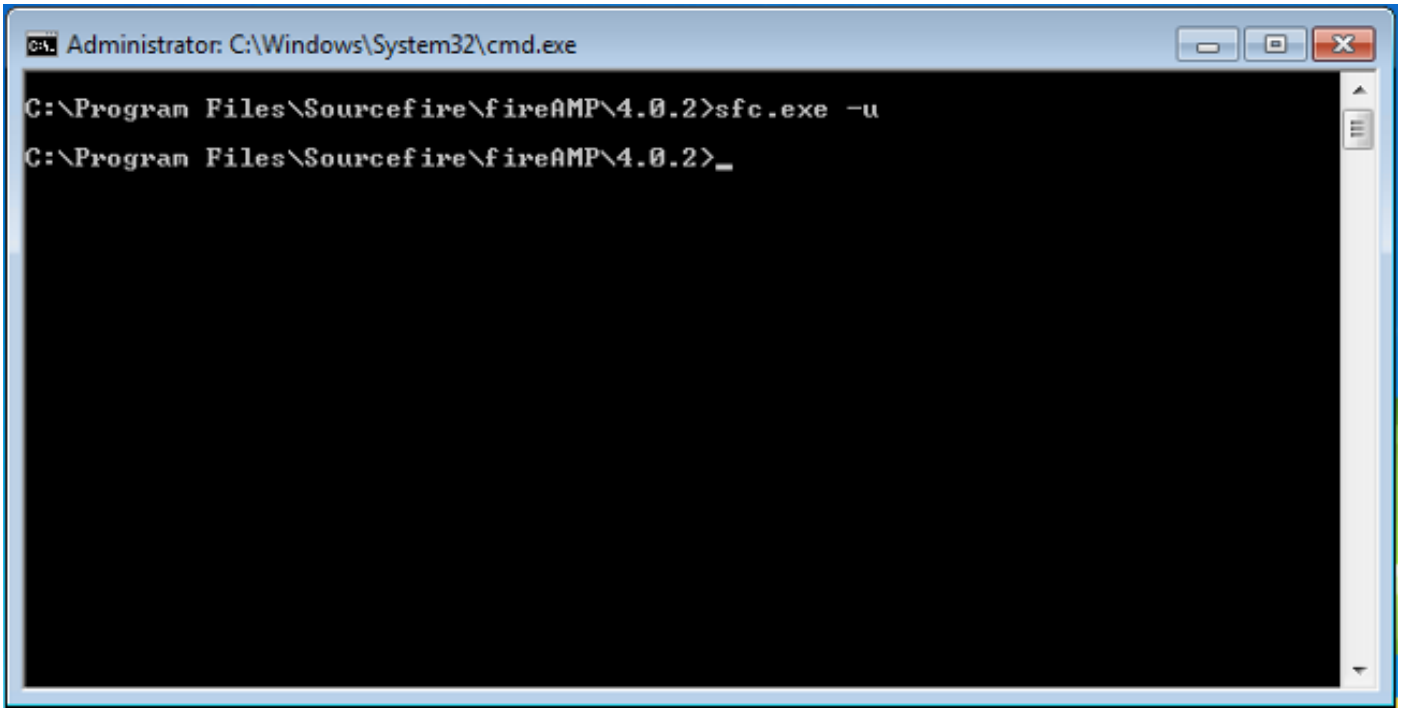
```
net stop immunetprotect
```



3. 确定fireAMP产品的位置。默认是`%PROGRAMFILES% \ Sourcefire \ fireAMP`

4. 通过运行`sfc.exe`卸载从控制面板的FireAMP连接器服务-版本文件夹的`u`。

```
"%PROGRAMFILES%\Sourcefire\fireAMP\4.0.2\sfc.exe" -u
```



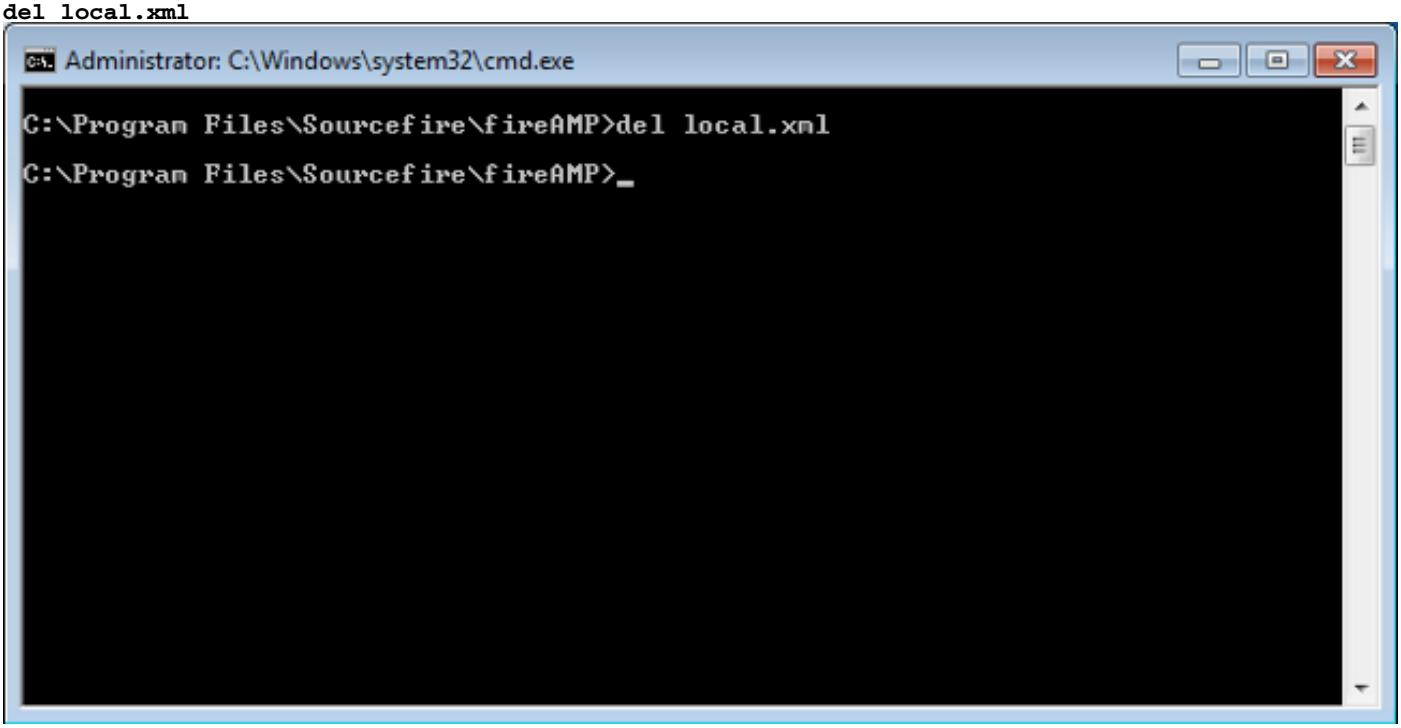
5. 如果要重新使用现有计算机对象，您必须备份现有`local.xml`。在以下目录local.xmlis ：

```
%PROGRAMFILES%\Sourcefire\fireAMP\
```

> **注意**：这对单个重新镜像是理想的，但是可能不是实用的为一对多的想象实践，因为存储唯一信息，例如单个的计算机的GUID。

6. 在您备份`local.xml`如果不需要重新使用在您的控制板的计算机对象，请删除local.xml

```
del local.xml
```



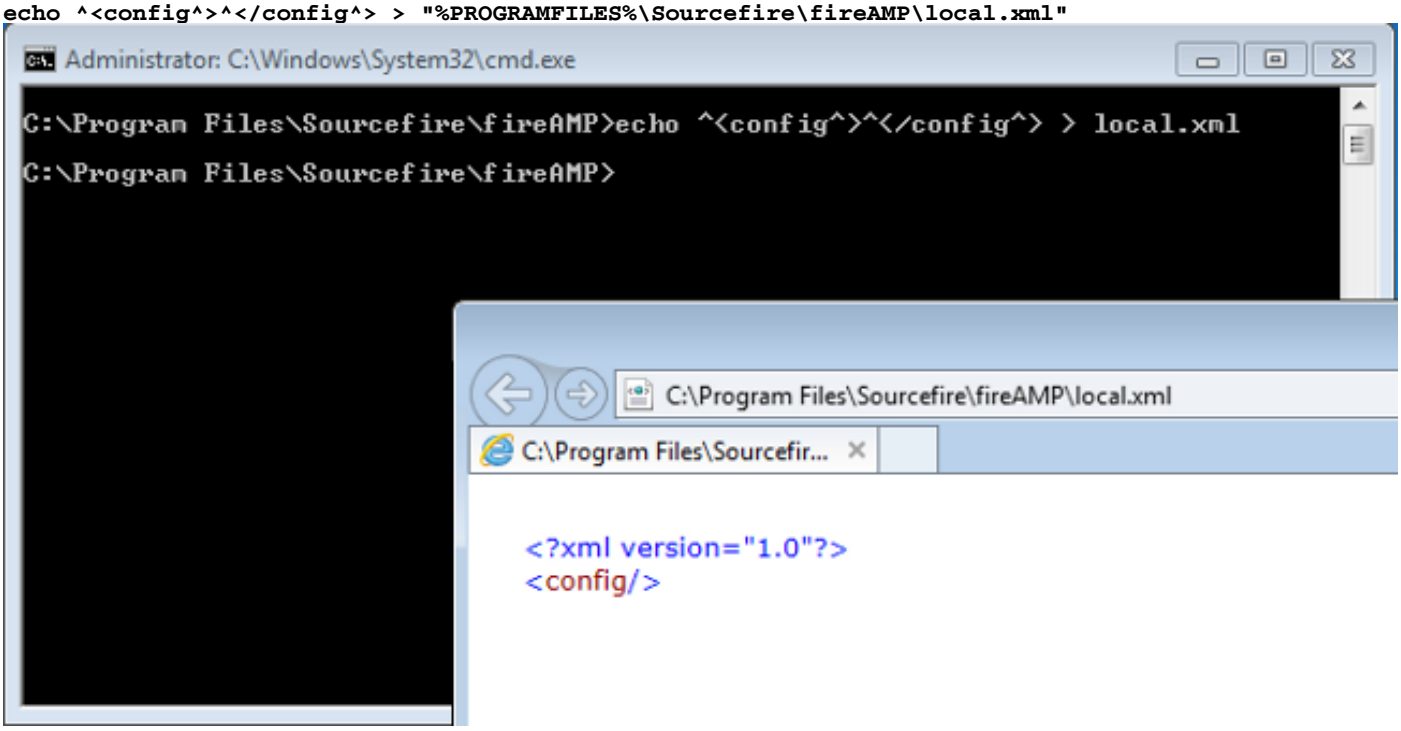
安装后

在部署您的镜像以后执行以下步骤：

注意：如果开始FireAMP服务用通用的`local.xml`，创建一个新的计算机对象。如果有原始local.xmlfile您能每台计算机恢复他们安排对象被重新使用。

1. 如果在重新映像之前，返回了它请恢复`local.xml`对此目录此时。如果不恢复local.xmlfile我们必须仍然创建一通用的一个连接器的能正确地注册。

```
echo ^<config^>^</config^> > "%PROGRAMFILES%\Sourcefire\fireAMP\local.xml"
```



2. 通过运行`SFC`注册有服务的连接器-从版本文件夹的`r`。此步骤完成计算机的`local.xml`。

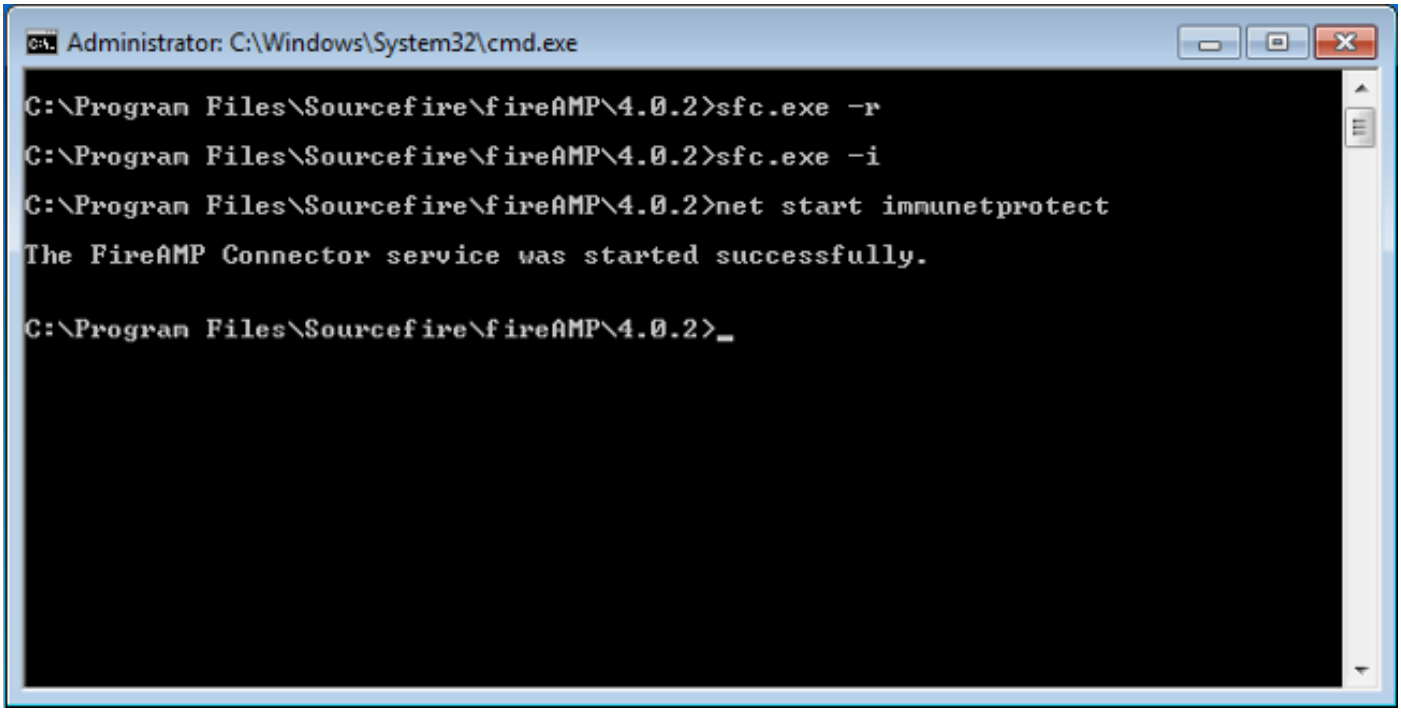
```
"%PROGRAMFILES%\Sourcefire\fireAMP\4.0.2\sfc.exe" -r
```

安装连接器对服务控制面板通过运行`sfc.exe -`版本文件夹的`i`。

```
"%PROGRAMFILES%\Sourcefire\fireAMP\4.0.2\sfc.exe" -i
```

通过运行命令启动连接器：

```
net start immunetprotect
```



这时FireAMP客户端应该是正在运行的。您能使用网页用户界面验证连接，并且服务运行的那。

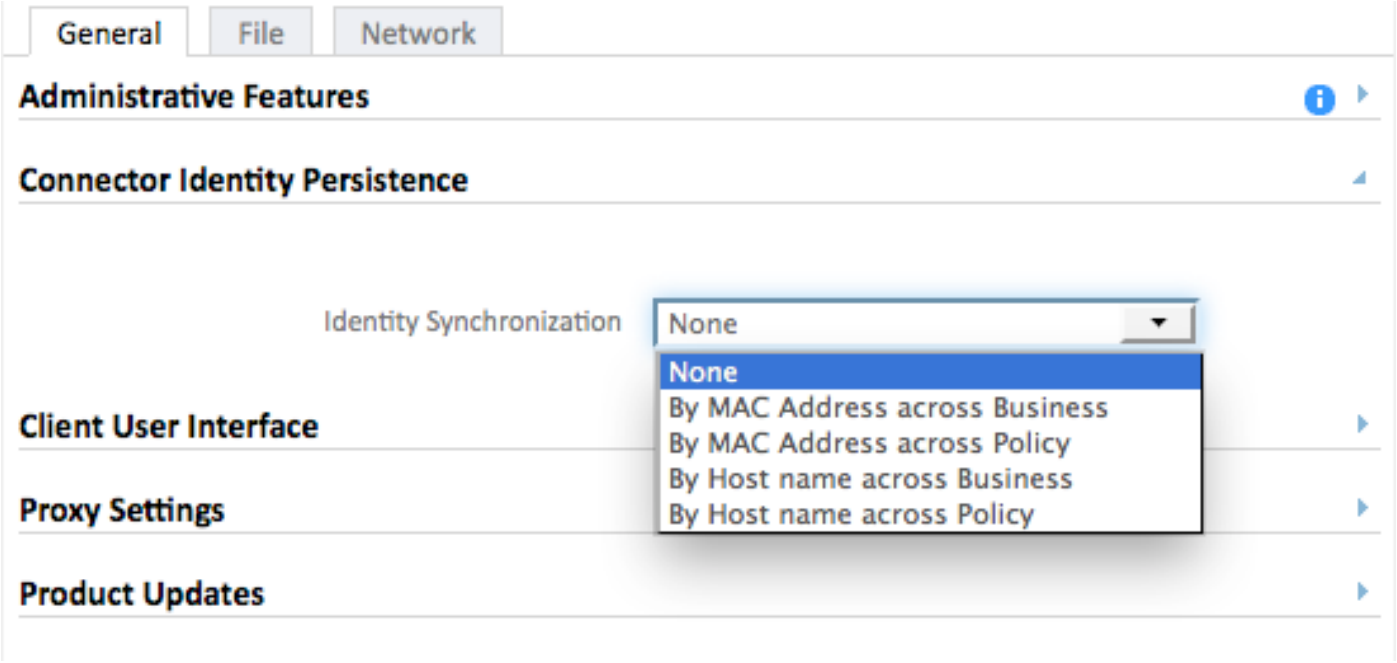
标识同步

标识同步允许您维护一一致事件登录虚拟环境或，当计算机被再镜像。您能绑定连接器到MAC地址或主机名，以便新的事件日志每次没有创建新的虚拟会话开始或计算机被再镜像。您能选择应用与粒度的此设置在不同的策略间，或者在您的整个组织间。

注意：有时被克隆从的一台被克隆的虚拟机可能在默认组中安置而不是组。如果这发生，请搬

入虚拟机正确组在FireAMP控制台。

为了启用标识同步，您需要配置您要适用于您的计算机的策略。



因为您能测试和控制环境的方面标识同步在实验室环境工作良好。然而，它有几个限制：

- 标识同步通过有代理程序版本的4.1.x代理只运作和以后。
- 标识同步由单个MAC地址同步。 那含义，如果有与有线的和无线卡的一笔记本电脑，您可能获得在网云的两标识。
- 标识同步由完全限定域名同步。 那含义，如果有一个DHCP服务器给您的标识可能不更改的网域字尾的。
- 在您的在最初的安装的策略必须配置标识同步。 如果启用标识同步安装后，则您可以最终获得重复项。