Отобразите или клонируйте компьютер с установленным разъёмом FireAMP

Содержание

Введение

Этот документ описывает процессы для предотвращения нескольк компьютеров для попытки использования того же Глобально уникального идентификатора (GUID), который предотвращает двойные компьютерные объекты для появления в облачной информационной панели FireAMP. Этот процесс позволяет FireAMP работать должным образом на клонированную машину.

Как Системный администратор, можно хотеть включать разъём FireAMP на основных образах Компьютера с операционной системой Windows. FireAMP, однако, требует, чтобы могли быть однозначно определены системы. Общие действия для клонирования машины для Linux у основания этой статьи.

> **Примечание:** Первый набор инструкций применяется к версии 4.1.4 FireAMP или выше. Далее вы находите исходные шаги для машин рабочими более ранними версиями.

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

Настоящий документ не имеет жесткой привязки к каким-либо конкретным версиям программного обеспечения и оборудования.

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были

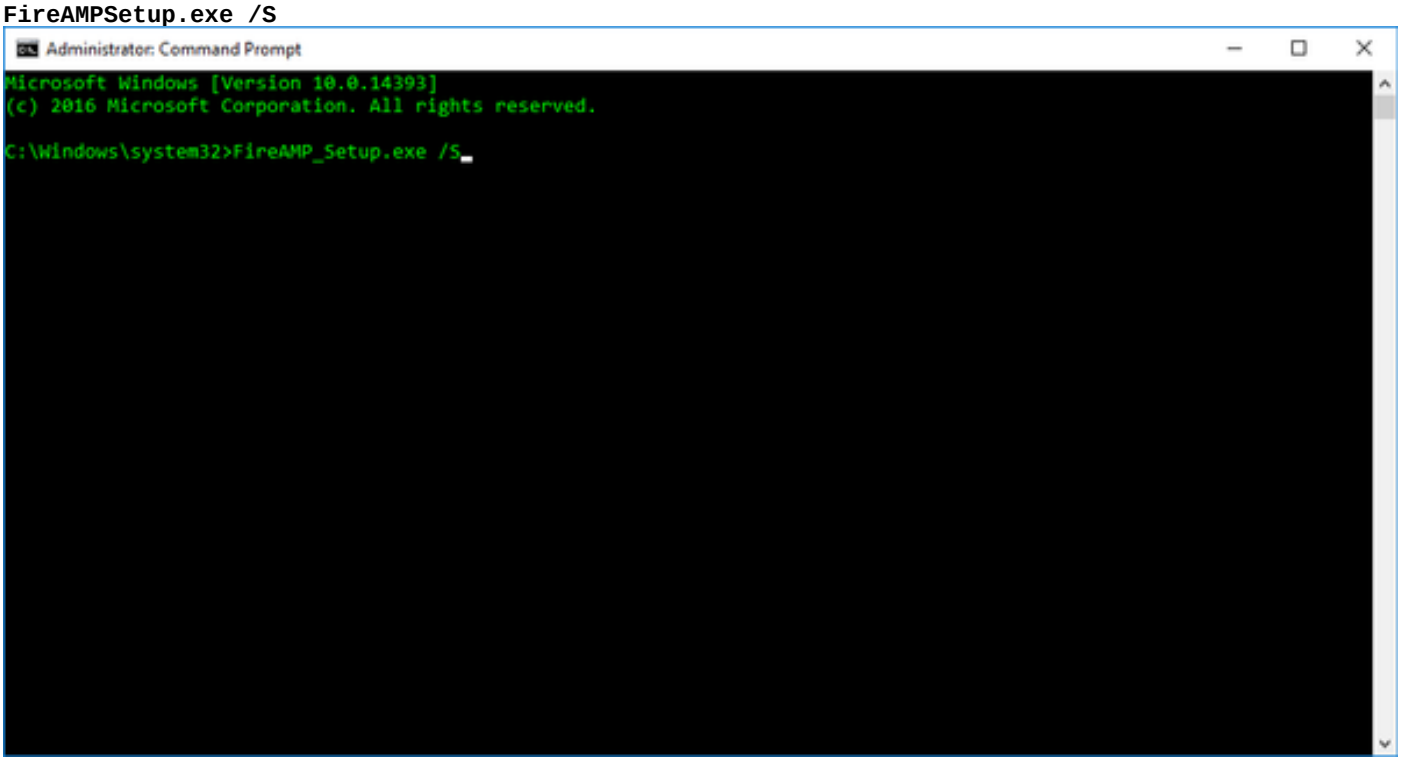
запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Предварительная установка - Версии 4.1.4 и выше

Выполните эти шаги для подготовки компьютера к обработке изображений:

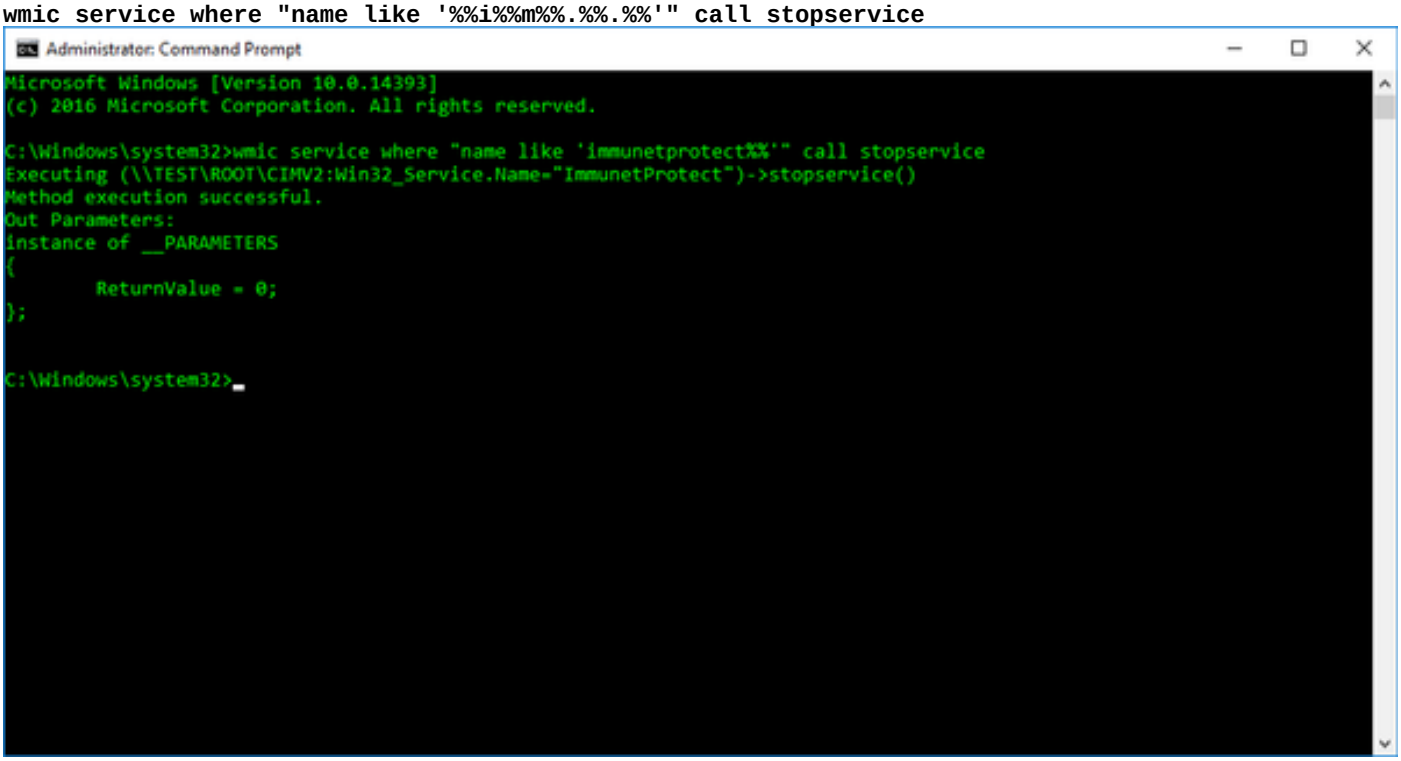
Шаг 1. Установите FireAMP на своем основном образе.

```
FireAMPSetup.exe /S
```



Шаг 2. Остановите сервис FireAMP.

```
wmic service where "name like '%%i%%m%%.%%.%%'" call stopservice
```



Используйте следующую команду, если вам включили защиту разъёма. Пароль будет видим в командной строке.

```
4.2 and Lower: Not Available
4.3 to 5.0: "%PROGRAMFILES%\Sourcefire\fireAMP\X.X.X\sfc.exe" -k protectionpassword
5.1 and Above: "%PROGRAMFILES%\Cisco\AMP\X.X.X\sfc.exe" -k protectionpassword
```

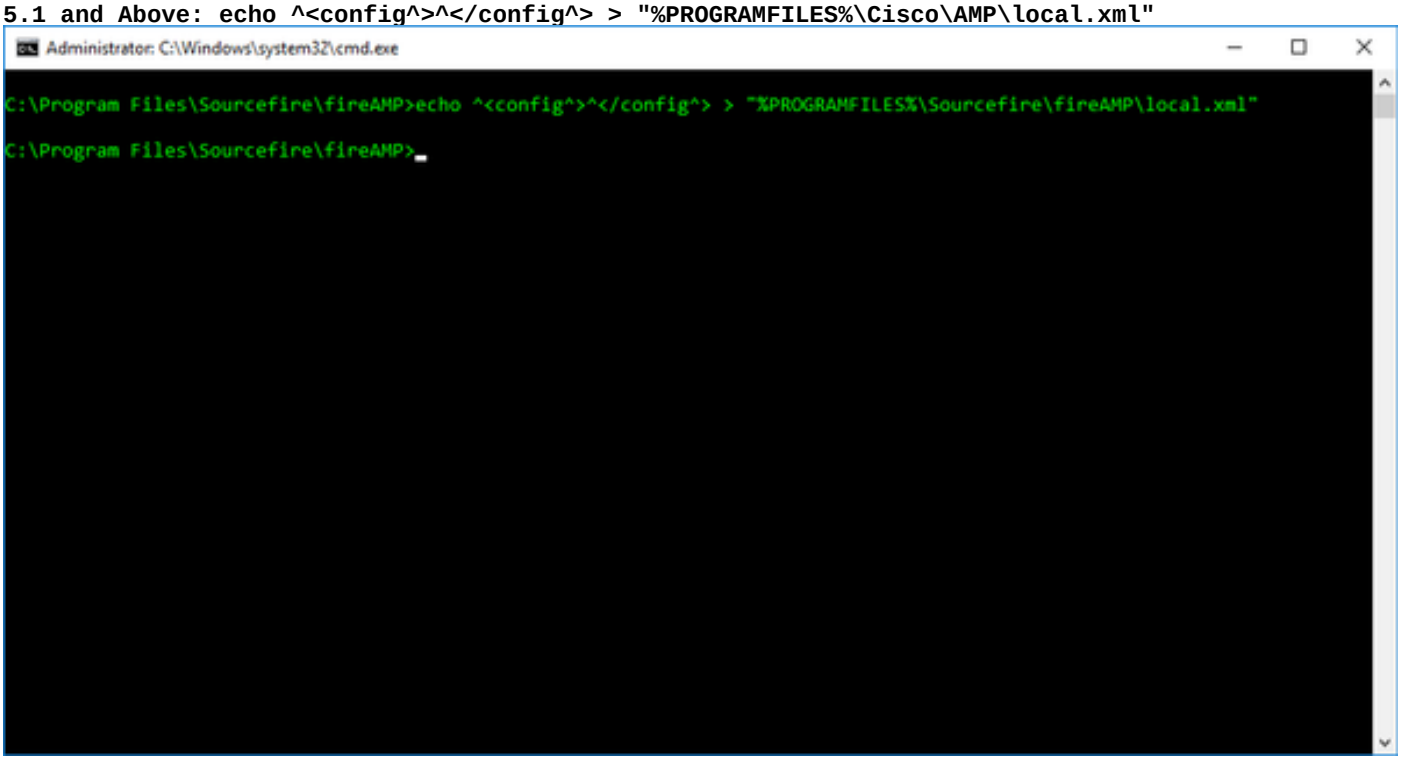
> **Примечание:** Если сервис FireAMP запущен снова, основной образ восстанавливает **local.xml**. Необходимо повторить эти шаги для нейтрализации основного образа снова. Обязательно включайте эти шаги в ваш основной процесс подготовки к образу.

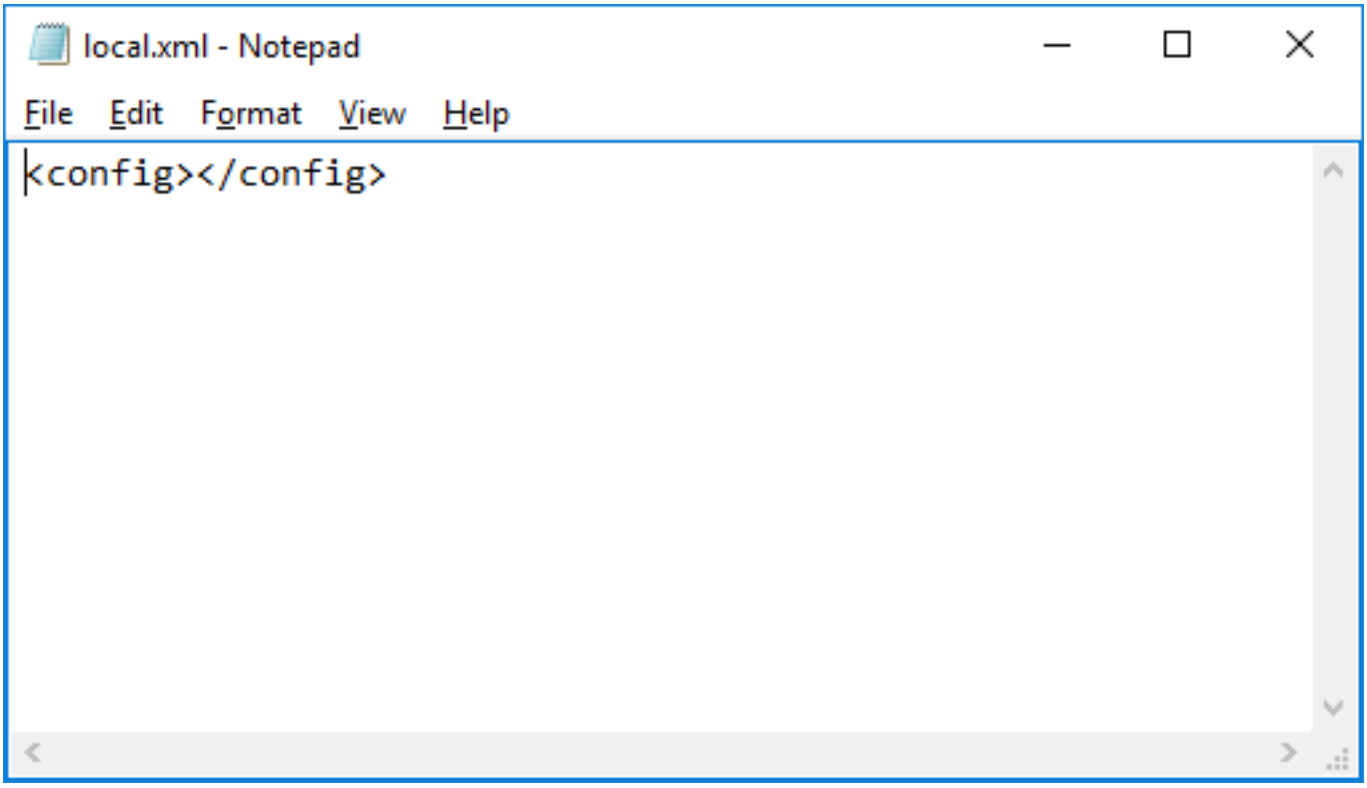
Шаг 3. Удалите **`local.xml`**.

```
5.0 and Lower: del "%PROGRAMFILES%\Sourcefire\fireAMP\local.xml"
5.1 and Above: del "%PROGRAMFILES%\Cisco\AMP\local.xml"
```

Шаг 4. . Создайте пробел **`local.xml`** файл.

```
5.0 and Lower: echo ^<config^>^</config^> > "%PROGRAMFILES%\Sourcefire\fireAMP\local.xml"
5.1 and Above: echo ^<config^>^</config^> > "%PROGRAMFILES%\Cisco\AMP\local.xml"
```





Постустановка - Версии 4.1.4 и выше

Когда сервис разъёма обнаруживает пробел **`local.xml`** файл, FireAMP 4.1.4 и выше автоматически генерирует новый regisration и Универсальный Уникальный идентификатор (UUID). Больше шагов не должно быть выполнено на самой машине.

> **Примечание:** Ожидается, что машины, которые регистрируют в пробеле **`local.xml`** файл, размещены в группу по умолчанию ваших организаций. Необходимо решить, хотите ли вы переместить эти машины вручную или изменить вашу группу по умолчанию, чтобы быть желаемой группой для тех машин.

На этом этапе клиент FireAMP должен быть в порядке. Можно использовать интерфейс пользователя для проверки подключения и что работает сервис. Если ваш интерфейс пользователя является "not set" для начала, это может быть вручную запущено с них, дают команду. Обязательно обновите номер версии для вашего в настоящее время установленная версия.

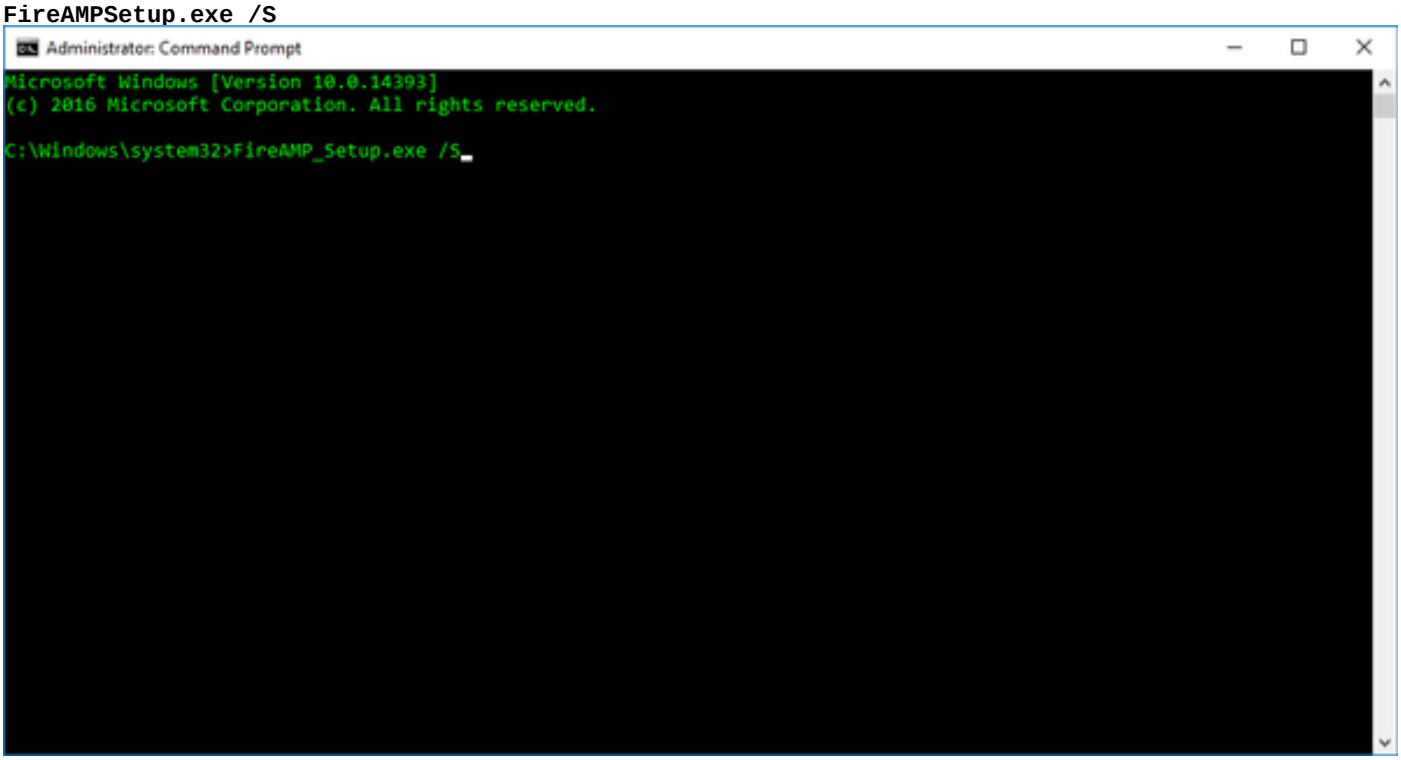
```
5.0 and Lower: "%PROGRAMFILES%\Sourcefire\fireAMP\X.X.X\iptray.exe" -f
5.1 and Above: "%PROGRAMFILES%\Cisco\AMP\X.X.X\iptray.exe" -f
```

Предварительная установка - Версии ниже, чем 4.1

Выполните эти шаги для подготовки компьютера к обработке изображений:

Шаг 1. Установите FireAMP на своем основном образе.

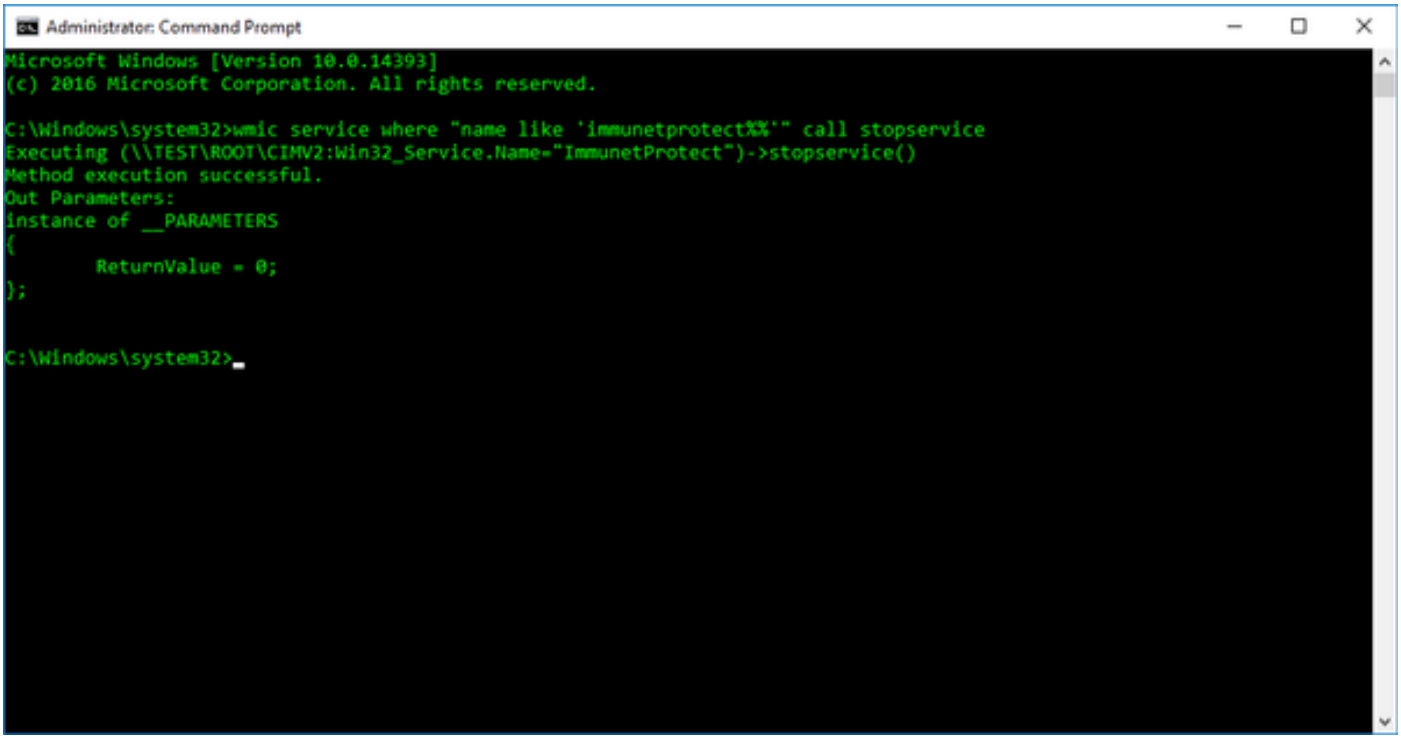
```
FireAMPSetup.exe /S
```



Шаг 2. Остановите сервис FireAMP.

> **Примечание:** При использовании пароля защиты разъёма это должно быть сделано от интерфейса пользователя.

```
wmic service where "name like '%%i%%m%%.%%.%%'" call stopservice
```



Шаг 3. Определите местоположение fireAMP продукта. По умолчанию

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

Шаг 4. . Деинсталлируйте Сервис Разъёма FireAMP от Панели управления путем выполнения **`sfc.exe-u`** от папки версии. Обязательно обновите команду с вашим в настоящее время номер установленной версии.

```
“%PROGRAMFILES%\Sourcefire\fireAMP\4.X.X\sfc.exe” -u
```

Шаг 5. . Если вы хотите снова использовать существующий компьютерный объект, необходимо резервировать существующий **`local.xml`** файл. **`local.xml`** найден в этом каталоге:

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

> **Примечание:** Это идеально для частного лица, повторно захватывают образ, но может не быть практичным для методов обработки изображений один ко многим, поскольку это хранит уникальную информацию, такую как GUID одиночного компьютера.

Шаг 6. После того, как вы выполняете резервное копирование **`local.xml`** или если вы не должны снова использовать компьютерный объект в своей информационной панели, удалите **`local.xml`**, :

```
del local.xml
```

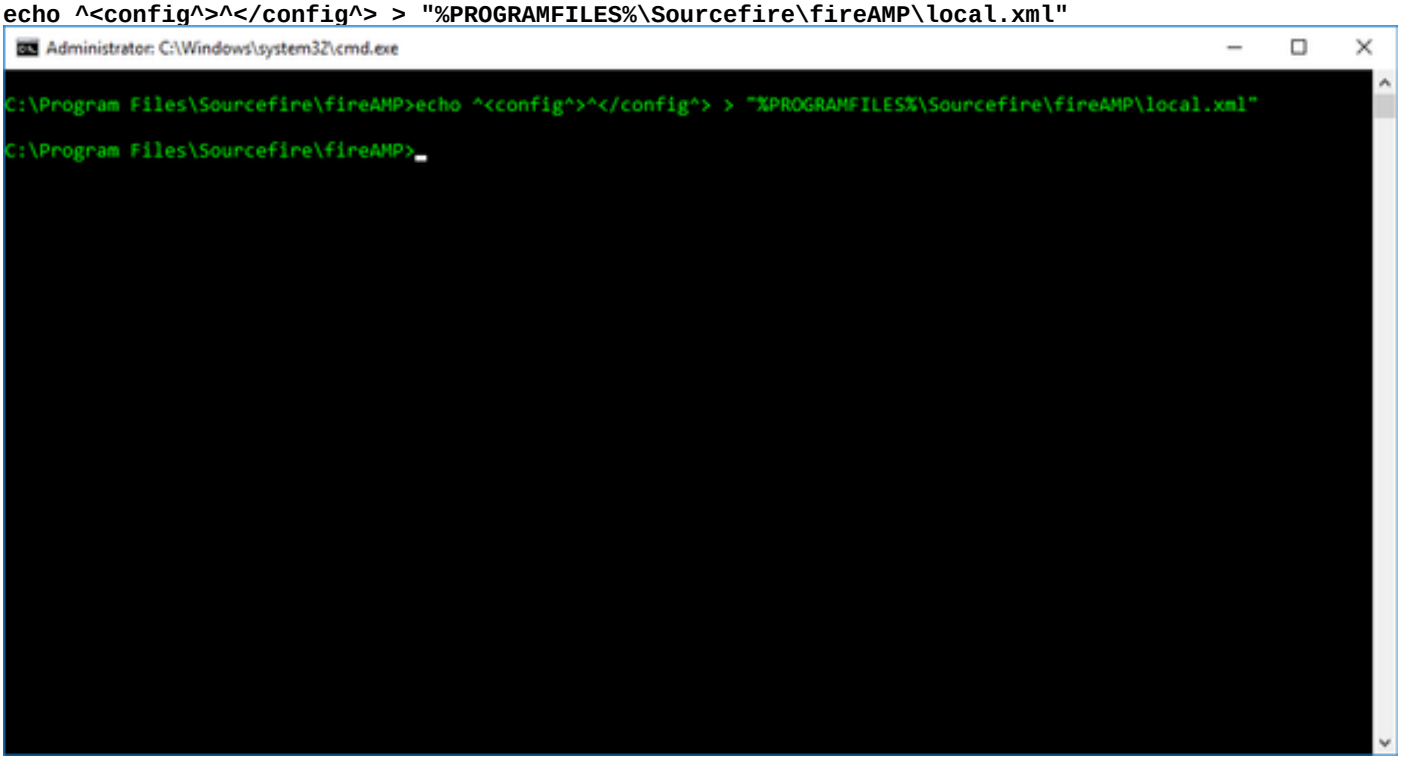
Постустановка - Версии ниже, чем 4.1

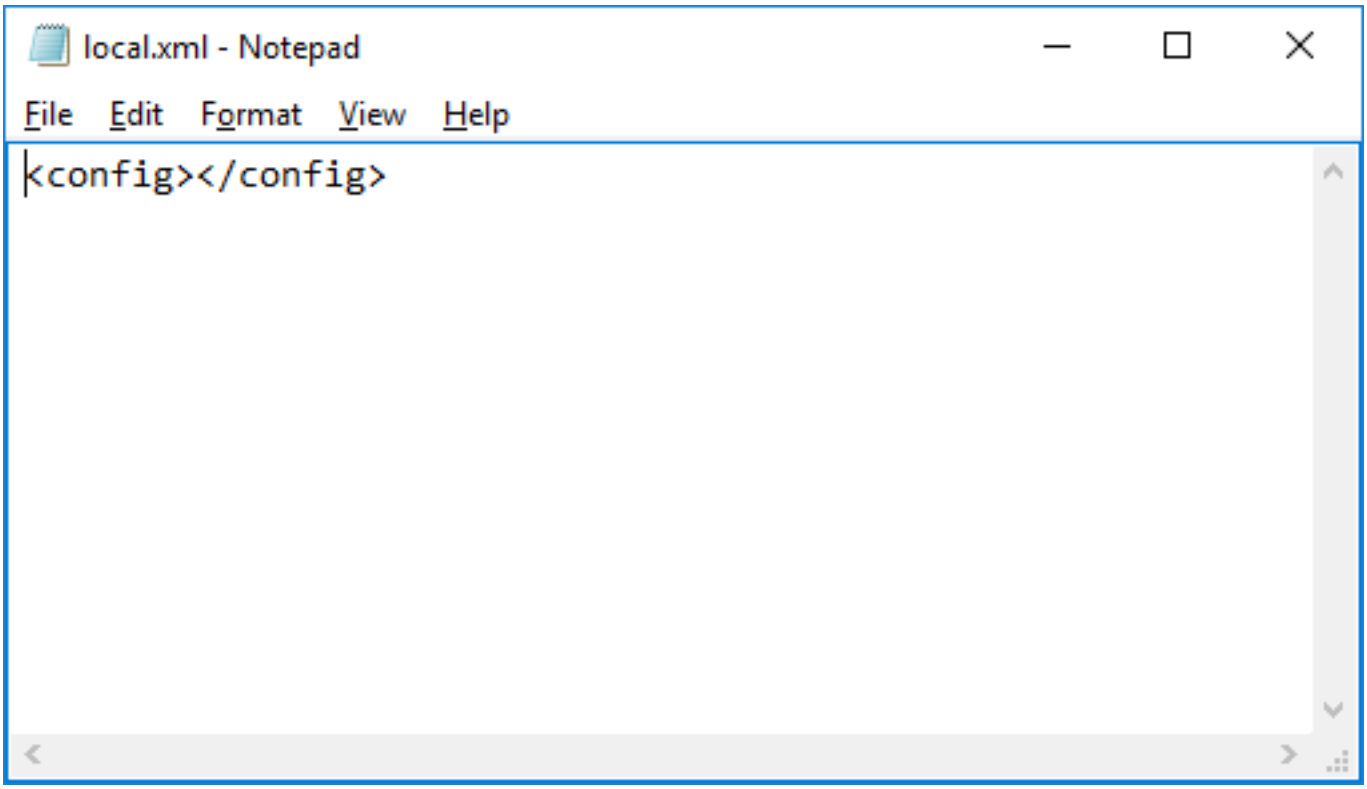
Выполните эти шаги после развертывания вашего образа:

> **Примечание:** При начале сервиса FireAMP с **`local.xml`** файла общего назначения он создает новый компьютерный объект. Если у вас есть исходный **`local.xml`** файл, можно восстановить их на компьютер, чтобы снова использовать объект.

Шаг 1. Восстановите **`local.xml`** файл к этому каталогу в это время при поддержке его до повторно захватывания образ. Если вы не восстанавливаете **`local.xml`** файл, необходимо все еще создать общего назначения для разъёма для регистрации правильно.

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





Шаг 2. Зарегистрируйте Разъём в сервисе путем выполнения **`sfc-r`** от папки версии. Этот шаг завершает **`local.xml`** файл для компьютера. Обязательно обновите ниже команд с вашим в настоящее время номер установленной версии.

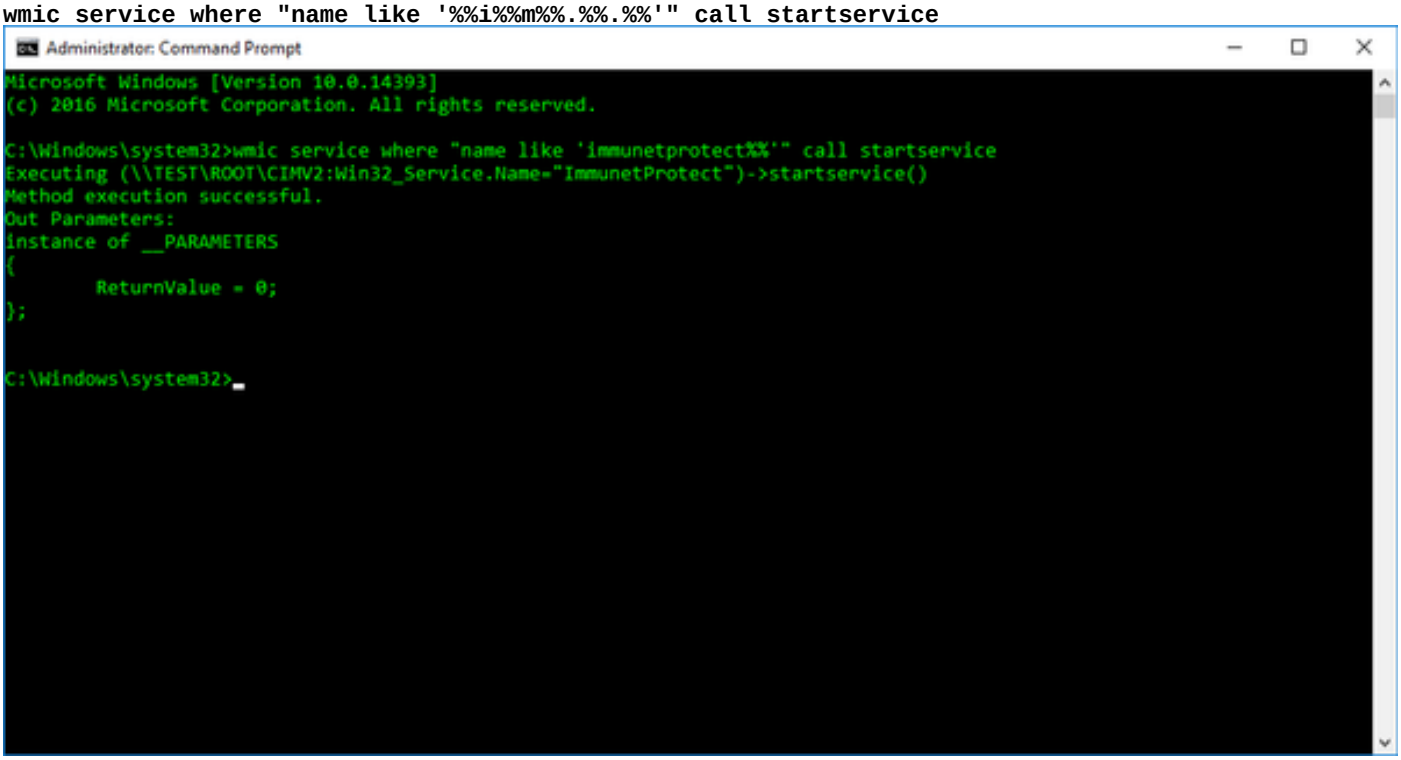
```
“%PROGRAMFILES%\Sourcefire\fireAMP\4.X.X\sfc.exe” -r
```

Установите Разъём к Панели управления Сервисов путем выполнения **`sfc.exe-i`** от папки версии.

```
“%PROGRAMFILES%\Sourcefire\fireAMP\4.X.X\sfc.exe” -i
```

Запустите Разъём путем выполнения команды:

```
wmic service where "name like '%%i%%m%%.%%.%%'" call startservice
```



> **Примечание:** Ожидается, что машины, которые вручную зарегистрированы таким образом, размещены в группу по умолчанию ваших организаций. Необходимо решить, хотите ли вы переместить эти машины вручную или изменить вашу группу по умолчанию, чтобы быть желаемой группой для тех машин.

На этом этапе клиент FireAMP должен быть в порядке. Можно использовать интерфейс пользователя для проверки подключения и что работает сервис. Если ваш интерфейс пользователя является "not set" для начала, это может быть вручную запущено с ниже команды. Обязательно обновите номер версии для вашего в настоящее время установленная версия.

```
"%PROGRAMFILES%\Sourcefire\fireAMP\4.X.X\iptray.exe" -f
```

Linux

Общие действия для клонирования машины для Linux и имеют новую идентичность, подобно Windows. Вот шаги и команды:

Установите AMP на своем основном образе

```
$ (sudo) yum install filename.rpm
```

Остановите сервис AMP

```
$ (sudo) initctl stop cisco-amp
```

Удалите local.xml

```
$ (sudo) rm /opt/cisco/amp/etc/local.xml
```

Когда другая машина загрузится с клонированным образом, сервис AMP будет автоматически запускать и генерировать новую идентичность. Это должно быть уникальный через все разъёмы передачи в группе в облаке [ли общественность, или частный].