Набор диагностических данных от разъёма FireAMP, работающего на Windows

Содержание

Введение

Этот документ описывает шаги для генерации файла диагностики от Разъёма FireAMP. Если вы испытываете техническую проблему с разъёмом FireAMP, который работает на Microsoft Windows, Инженер технической поддержки Cisco мог бы хотеть проанализировать сообщения журнала, доступные в файле диагностики.

Генерируйте файл диагностики

Зависящий от версии Windows, навигация к Инструменту диагностики Поддержки Разъёма FireAMP могла бы быть другой. В большинстве операционных систем Windows вы переходите к Меню Пуск для обнаружения Инструмента диагностики Поддержки Разъёма FireAMP. Пример:

Запустите> Все Программы> Разъём FireAMP> Инструмент диагностики Поддержки.

> **Примечание:** При запуске Windows с Управлением учетными записями пользователей нажмите **Yes**, чтобы позволить программному средству работать.

Инструмент диагностики Поддержки создает сжатый файл в 7z, форматируют, и сохраняет его на Рабочем столе. Вот пример имени файла файла диагностики на Рабочем столе:

v5.0 и ранее: `Sourcefire_Support_Tool_YYYY_MM_DD_HH_MM_SS.7z`

v5.1 и более новый: `CiscoAMP_Support_Tool_YYYY_MM_DD_HH_MM_SS.7z`

Также можно выполнить этот исполняемый файл как администратор:

```
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
```

Режим отладки

Включение режима отладки на разъёме FireAMP предоставляет дополнительное многословие регистрации, которая позволяет большее понимание проблем с разъёмом. В

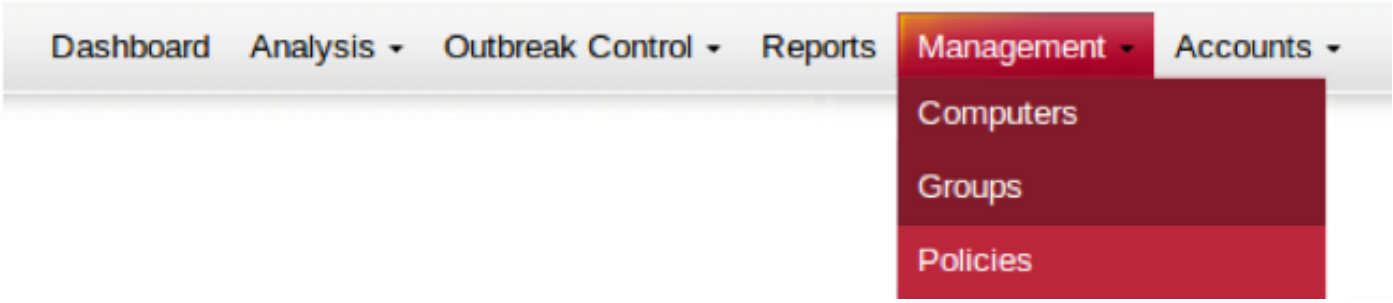
этом разделе описывается включить режим отладки в разъёме FireAMP.

> **% Warning:** Режим отладки должен быть включен, только если Инженер технической поддержки Cisco запрашивает эти данные. Включение режима отладки в течение более длинного времени может заполнить дисковое пространство очень быстро и могло бы препятствовать тому, чтобы Файл диагностики Поддержки собрал **Журнал Журнала** и **Лотка Разъёма** из-за чрезмерного размера файла.

Включите режим отладки

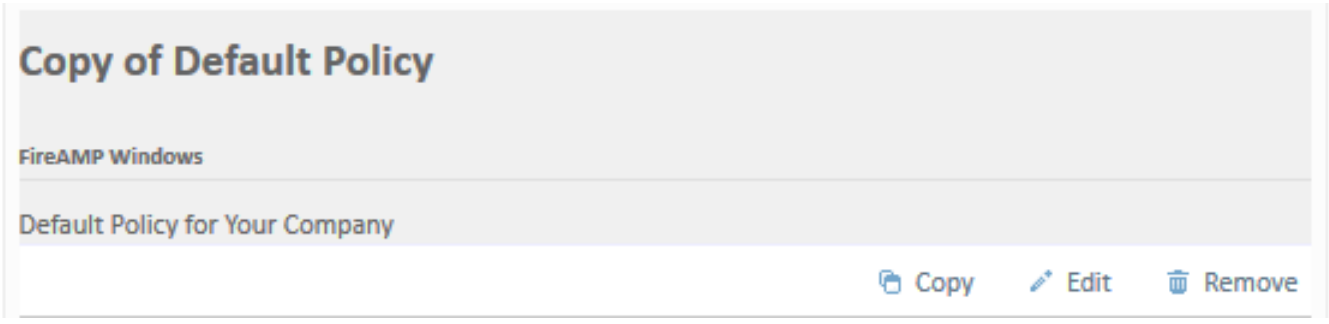
Шаг 1: Войдите в консоль FireAMP.

Шаг 2: Выберите **Managment> Policies**.

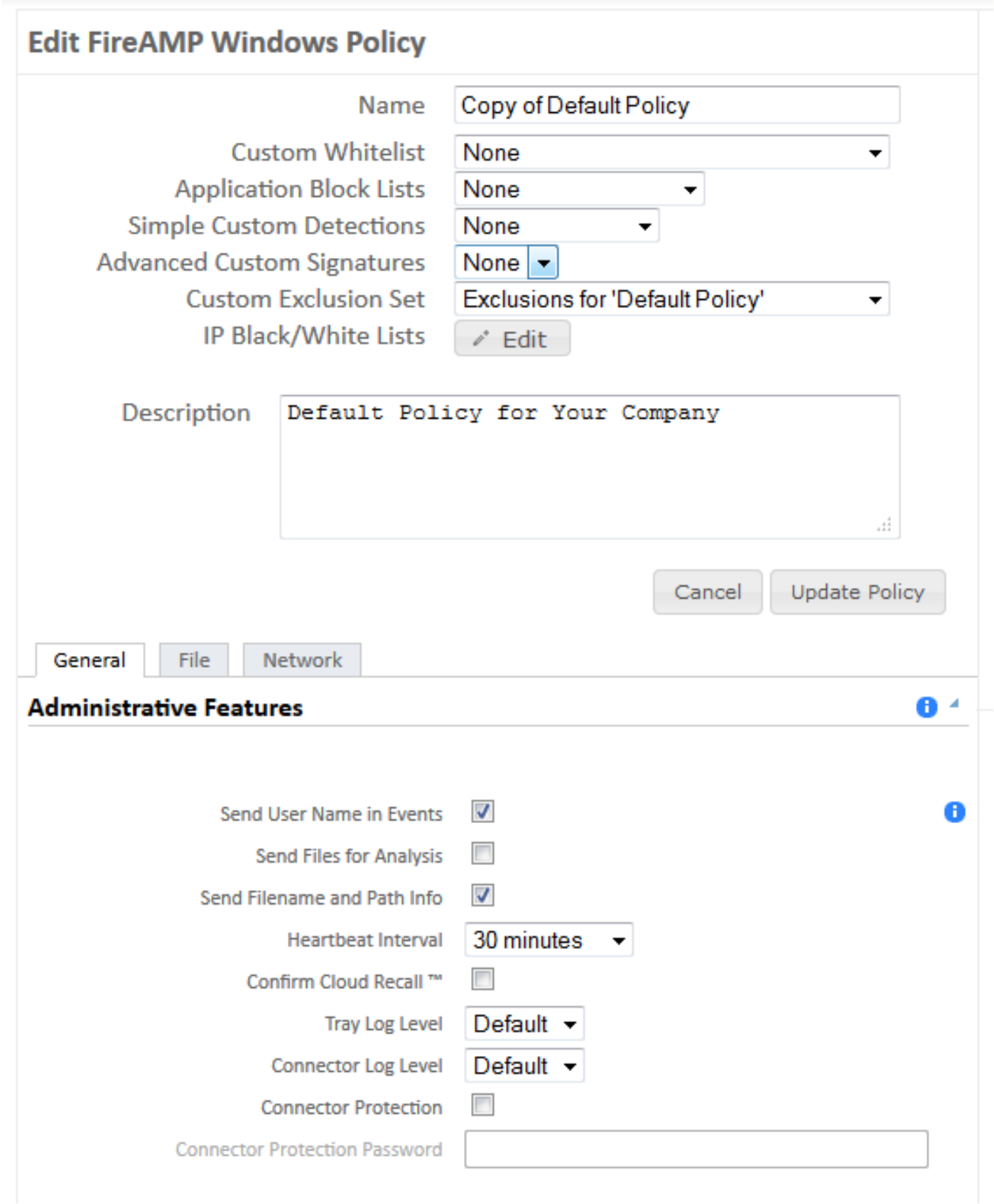


Шаг 3: Найдите Политику, которая применена к конечному устройству или компьютеру, и нажмите **Copy.**

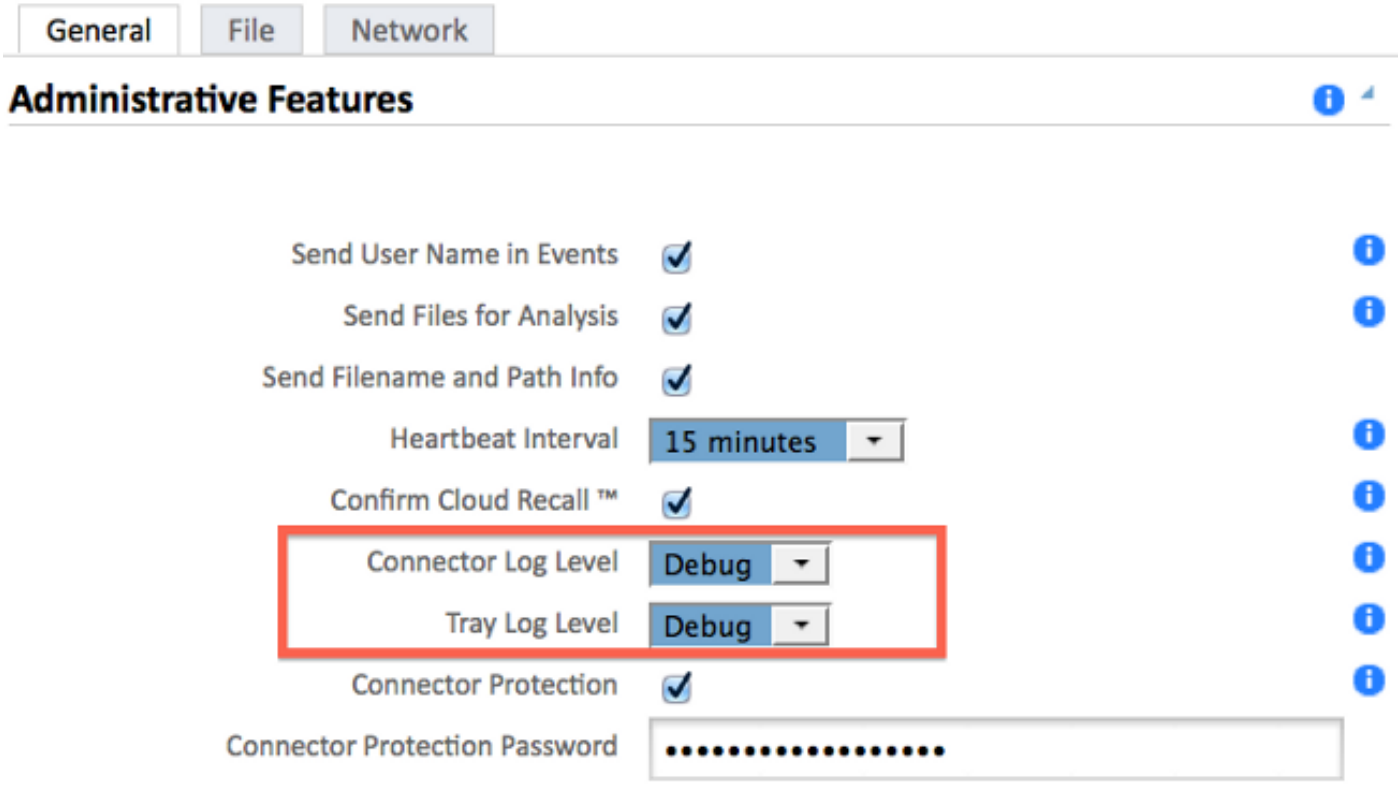
Шаг 4. : После нажатия Copy, обновлений Консоли FireAMP со скопированной политикой.



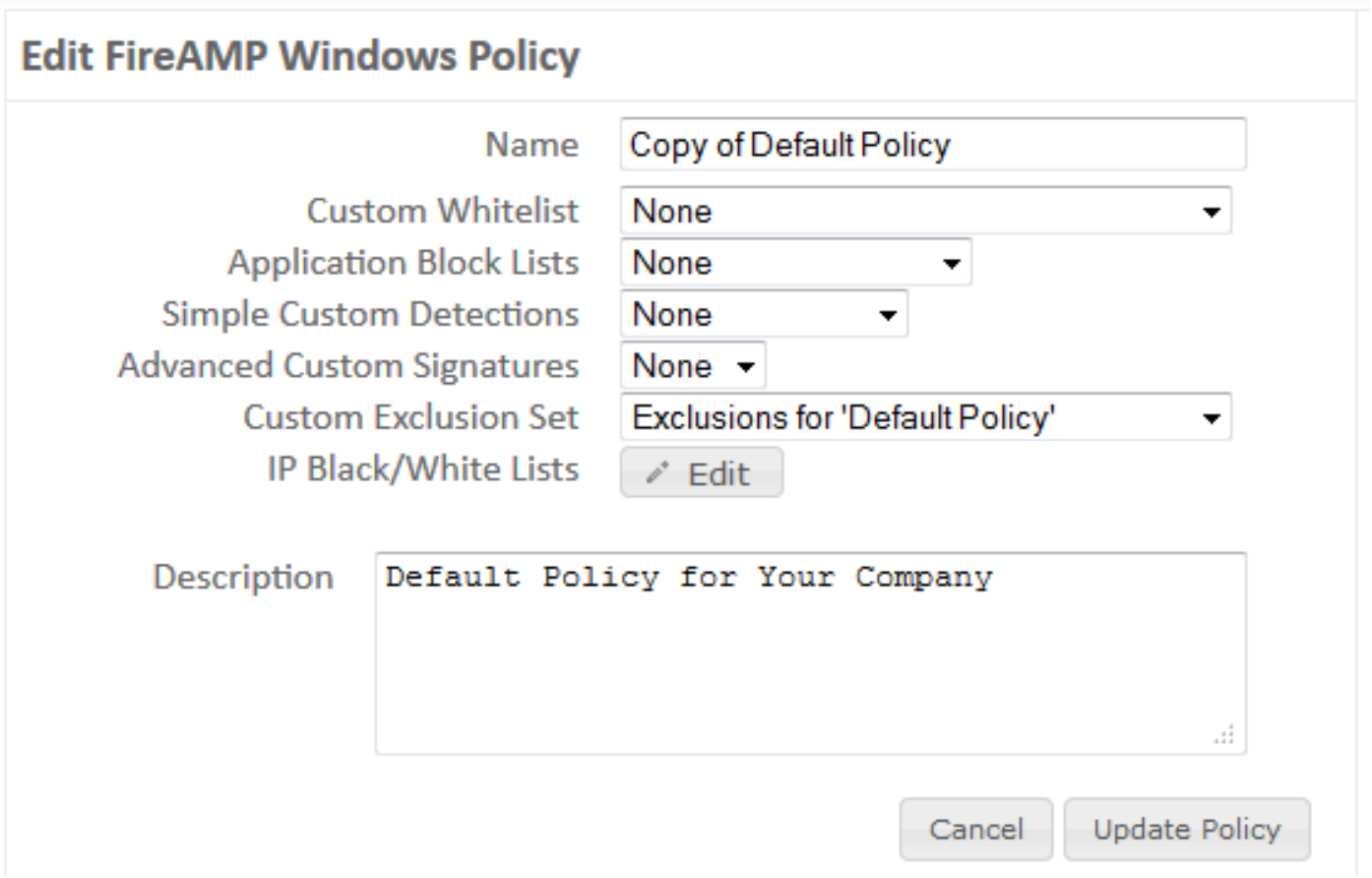
Шаг 5. : Нажмите **Edit** и затем нажмите **Administrative Features**.



Шаг 6: Для **Уровня Журнала Уровня** и **Разъёма Журнала Лотка** выберите **Debug** из выпадающих списков.



Шаг 7: Нажмите **Update Policy** для сохранения изменений.

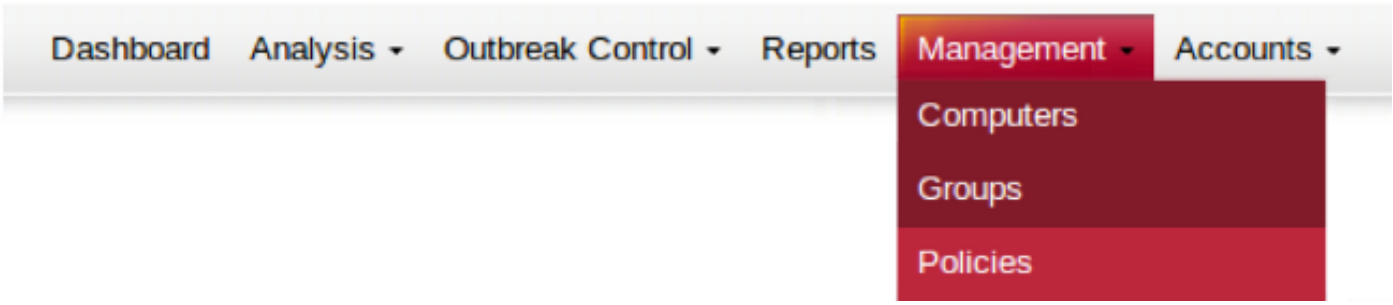


Шаг 8: После обновления политики необходимо применить это на конечное устройство, где вы хотите генерировать отладочную информацию.

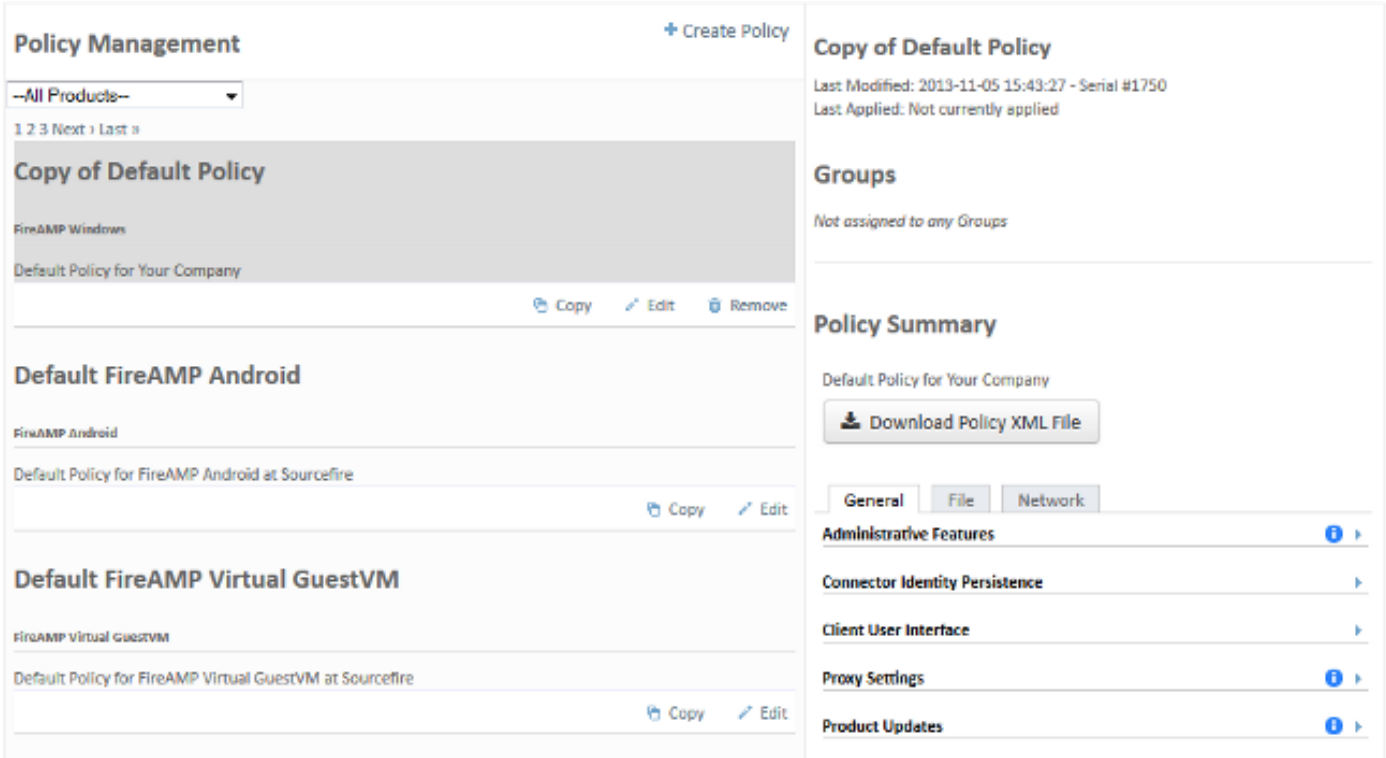
Неспособный включить режим отладки

Из-за проблемы с подключением, если вы неспособны применить политику к Разъёму FireAMP, вы будете неспособны включить режим отладки. В этом случае можно загрузить `policy.xml` файл и настроить Разъём FireAMP для использования модифицированной политики. Следуйте этим инструкциям, если облако FireAMP неспособно связаться с разъёмом FireAMP:

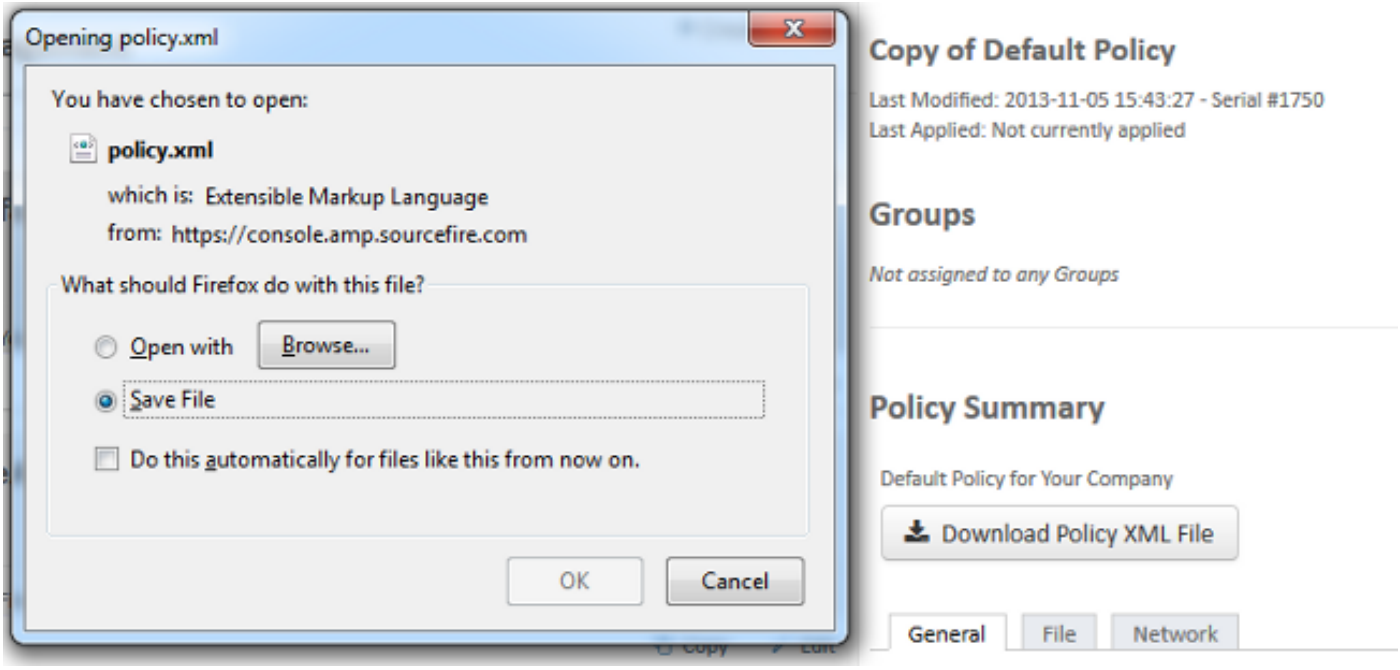
Шаг 1: Выберите **Management> Policies**.



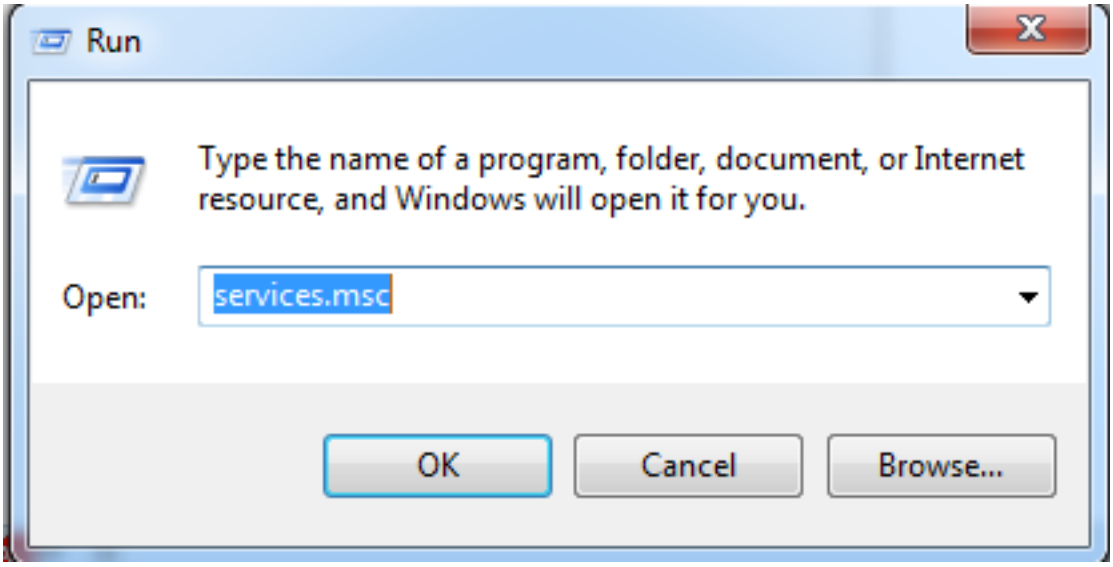
Шаг 2: Найдите Политику, которая была скопирована, и щелкните по названию для отображения **Сводки Политики**.



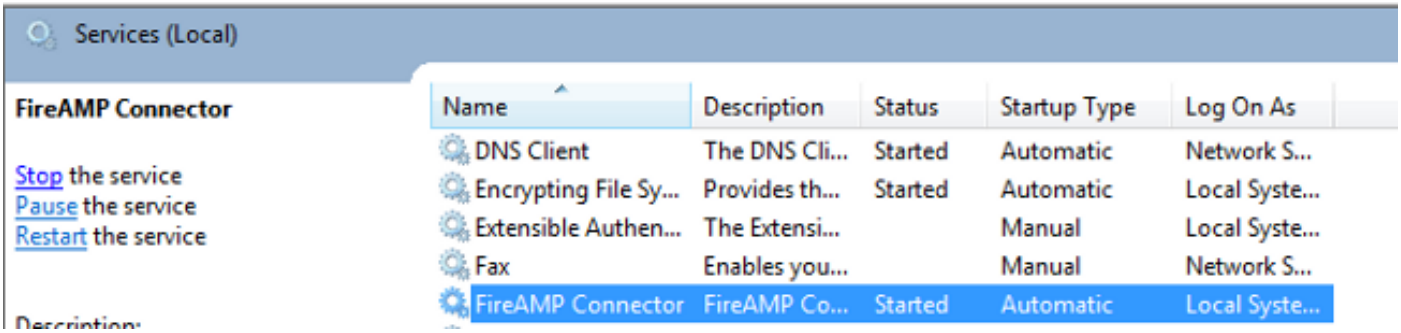
Шаг 3: Нажмите **Download Policy XML File** и затем сохраните файл к своему компьютеру.



Шаг 4. : Откройте **`services.msc`** с **Пуском> Выполнить**.



Шаг 5. : Найдите сервис **Разъёма FireAMP** и нажмите **Stop**.



Шаг 6: Нажмите **Start> Computer**, затем перейдите к одному из этих каталогов в зависимости от архитектуры ЭВМ:

В x86 Платформе:

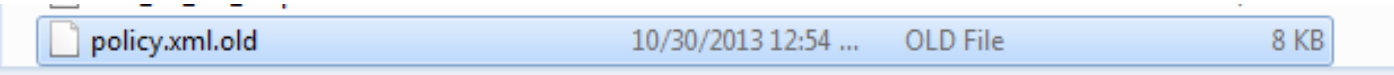
```
v5.0 and earlier: C:\Program Files (x86)\Sourcefire\fireAMP
```

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

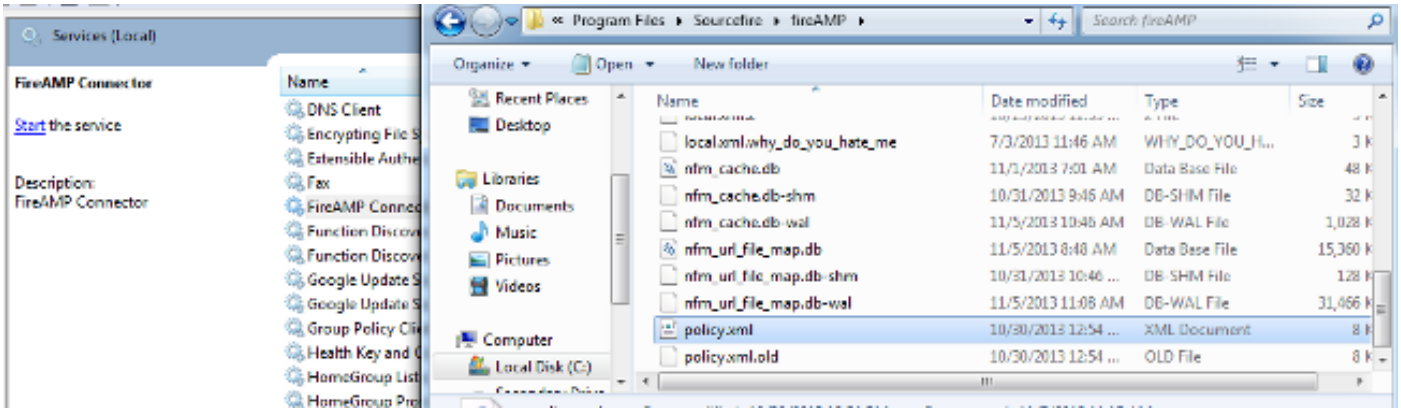
В x64 Платформе:

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

Шаг 7: Найдите файл `policy.xml` и переименуйте файл к `policy.xml.old`.



Шаг 8: Переместите загруженный `policy.xml` в каталог и затем нажмите **Start сервис** в окне Services. Разъём FireAMP находится теперь в режиме отладки и регистрирует дополнительные диагностические данные.



Для отключения режима отладки выполните Шаг 5 посредством Шага 8, отмените изменения к `policy.xml.old` и перезапустите Разъём FireAMP.