

Набор диагностических данных от разъёма FireAMP, работающего на Windows

Содержание

[Введение](#)

[Генерируйте файл диагностики](#)

[Режим отладки](#)

[Включите режим отладки](#)

[Неспособный включить режим отладки](#)

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

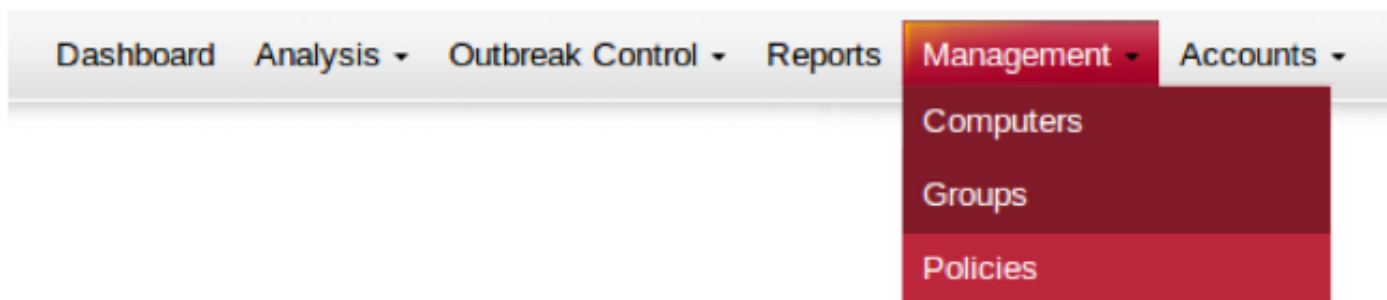
этом разделе описывается включить режим отладки в разъёме FireAMP.

% 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.

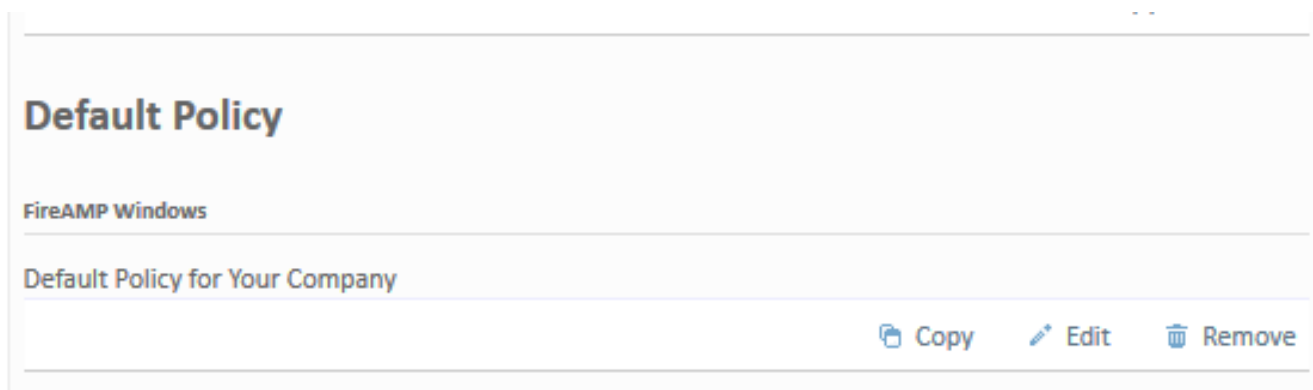
Включите режим отладки

Шаг 1: Войдите в консоль FireAMP.

Шаг 2: Выберите **Management > 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**.

Edit FireAMP Windows Policy

Name	<input type="text" value="Copy of Default Policy"/>
Custom Whitelist	<input type="text" value="None"/>
Application Block Lists	<input type="text" value="None"/>
Simple Custom Detections	<input type="text" value="None"/>
Advanced Custom Signatures	<input type="text" value="None"/>
Custom Exclusion Set	<input type="text" value="Exclusions for 'Default Policy'"/>
IP Black/White Lists	<input type="button" value="Edit"/>

Description

Cancel

Update Policy

General

File

Network

Administrative Features

Send User Name in Events	<input checked="" type="checkbox"/>	
Send Files for Analysis	<input type="checkbox"/>	
Send Filename and Path Info	<input checked="" type="checkbox"/>	
Heartbeat Interval	<input type="text" value="30 minutes"/>	
Confirm Cloud Recall™	<input type="checkbox"/>	
Tray Log Level	<input type="text" value="Default"/>	
Connector Log Level	<input type="text" value="Default"/>	
Connector Protection	<input type="checkbox"/>	
Connector Protection Password	<input type="text"/>	

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

General

File

Network

Administrative Features



Send User Name in Events	<input checked="" type="checkbox"/>	
Send Files for Analysis	<input checked="" type="checkbox"/>	
Send Filename and Path Info	<input checked="" type="checkbox"/>	
Heartbeat Interval	15 minutes	
Confirm Cloud Recall™	<input checked="" type="checkbox"/>	
Connector Log Level	Debug	
Tray Log Level	Debug	
Connector Protection	<input checked="" type="checkbox"/>	
Connector Protection Password	

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

Edit FireAMP Windows Policy

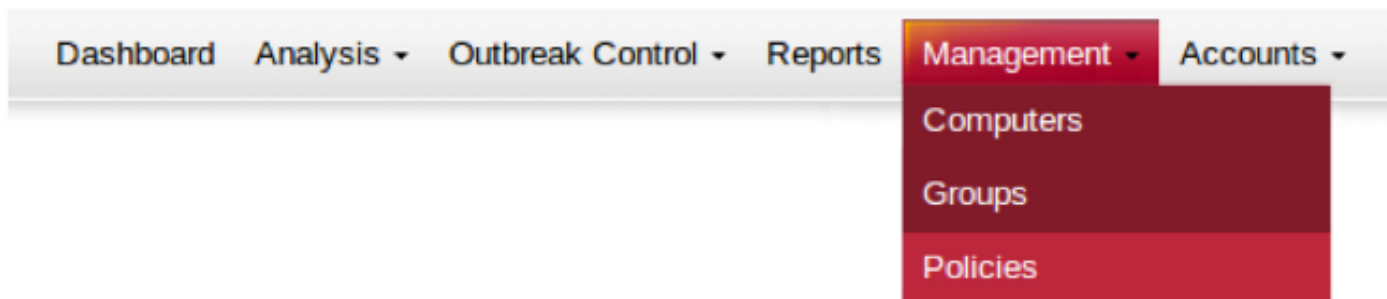
Name	Copy of Default Policy
Custom Whitelist	None
Application Block Lists	None
Simple Custom Detections	None
Advanced Custom Signatures	None
Custom Exclusion Set	Exclusions for 'Default Policy'
IP Black/White Lists	Edit
Description	Default Policy for Your Company

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:

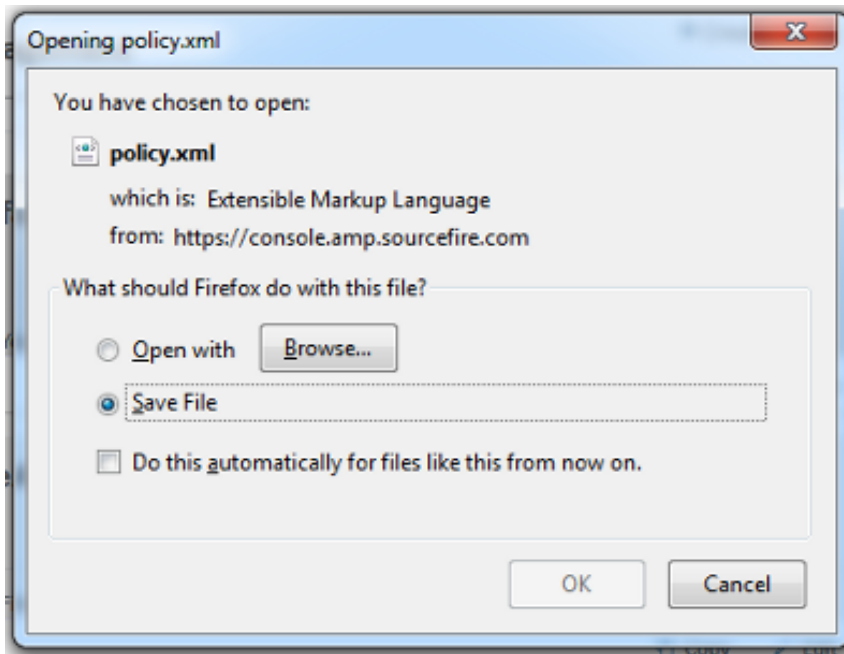
Шаг 1: Выберите **Management** > **Policies**.



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

A screenshot of the FireAMP Policy Management interface. The left pane shows a list of policies under 'Policy Management'. The right pane shows the details for a selected policy, 'Copy of Default Policy'. The details include a 'Download Policy XML File' button and a 'Policy Summary' section with tabs for 'General', 'File', and 'Network'. The 'General' tab is active, showing sections for 'Administrative Features', 'Connector Identity Persistence', 'Client User Interface', 'Proxy Settings', and 'Product Updates'.

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



Copy of Default Policy

Last Modified: 2013-11-05 15:43:27 - Serial #1750
Last Applied: Not currently applied

Groups

Not assigned to any Groups

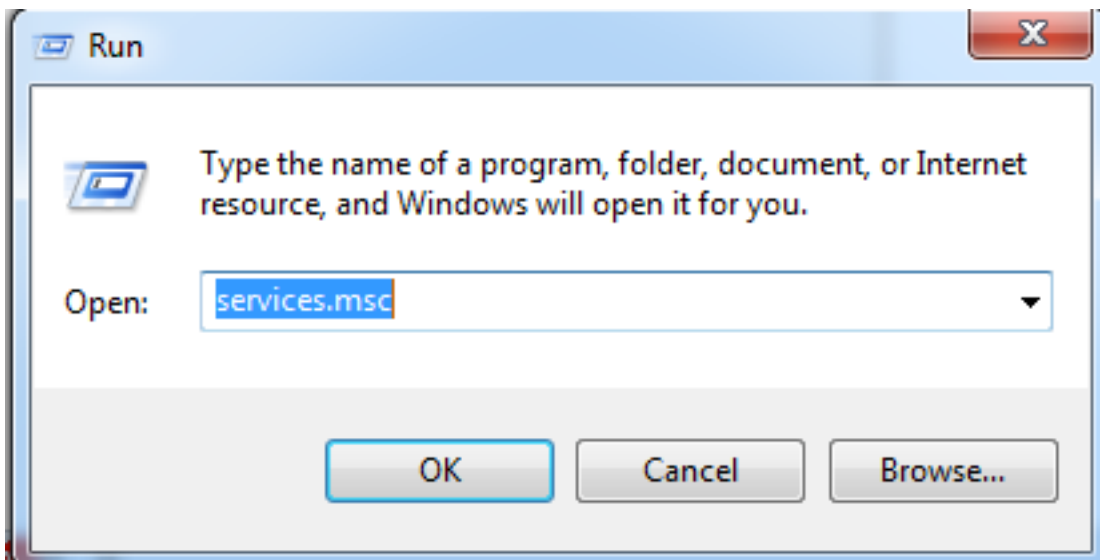
Policy Summary

Default Policy for Your Company

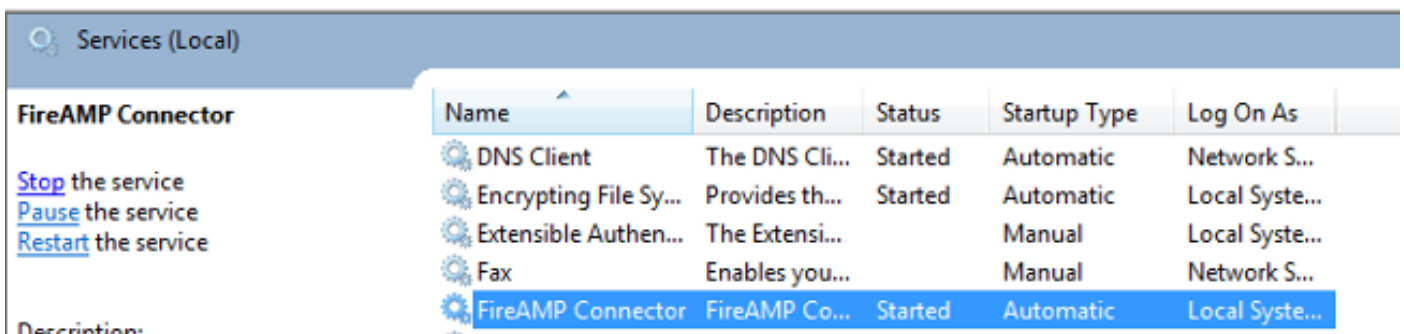
[Download Policy XML File](#)

General File Network

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

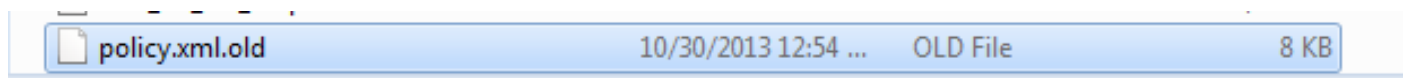
v5.1 and newer: C:\Program Files (x86)\Cisco\AMP

В x64 Платформе:

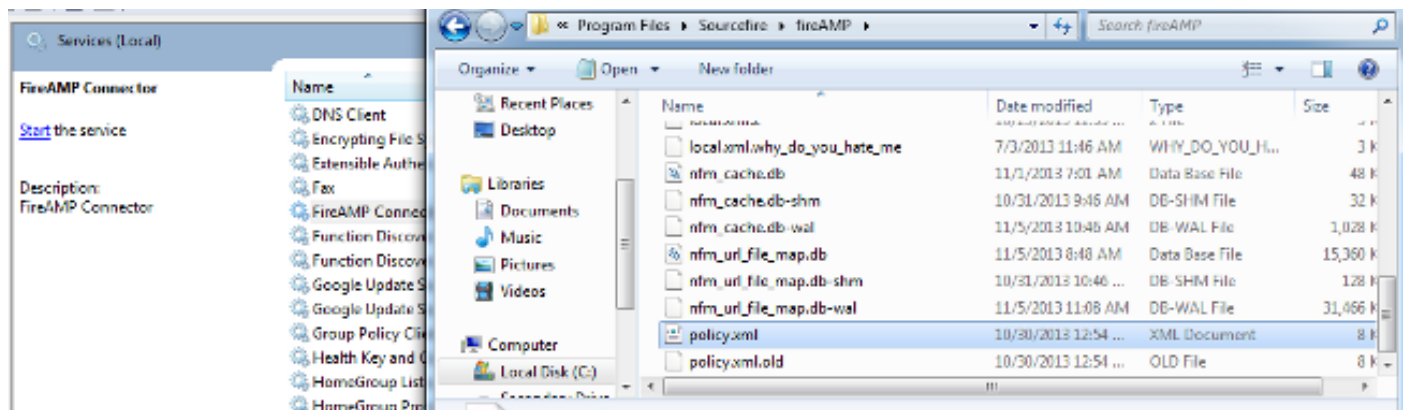
v5.0 and earlier: C:\Program Files\Sourcefire\fireAMP

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.