Разъём FireAMP для набора диагностических данных Mac

Содержание

Введение

Этот документ описывает процесс, который используется для генерации файла диагностики с помощью приложения Инструмента поддержки, которое доступно на Разъёме Cisco FireAMP для Macintosh (Mac) машины и как устранить неполадки проблем производительности.

Предварительные условия

Требования

Компания Cisco рекомендует предварительно ознакомиться со следующими предметами:

- Разъём Cisco FireAMP для Mac
- Mac OS X

Используемые компоненты

Сведения в этом документе основываются на Разъёме Cisco FireAMP для Mac.

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.

Общие сведения

Разъём Cisco FireAMP для Mac устанавливает приложение под названием *Инструмент поддержки*, который используется для генерации диагностической информации о Разъёме FireAMP, который установлен на Mac. Диагностические данные включают информацию о вашем Mac, таком как:

- Использование ресурса (диск, ЦП и память)
- FireAMP-специфичные журналы
- Сведения о конфигурации FireAMP

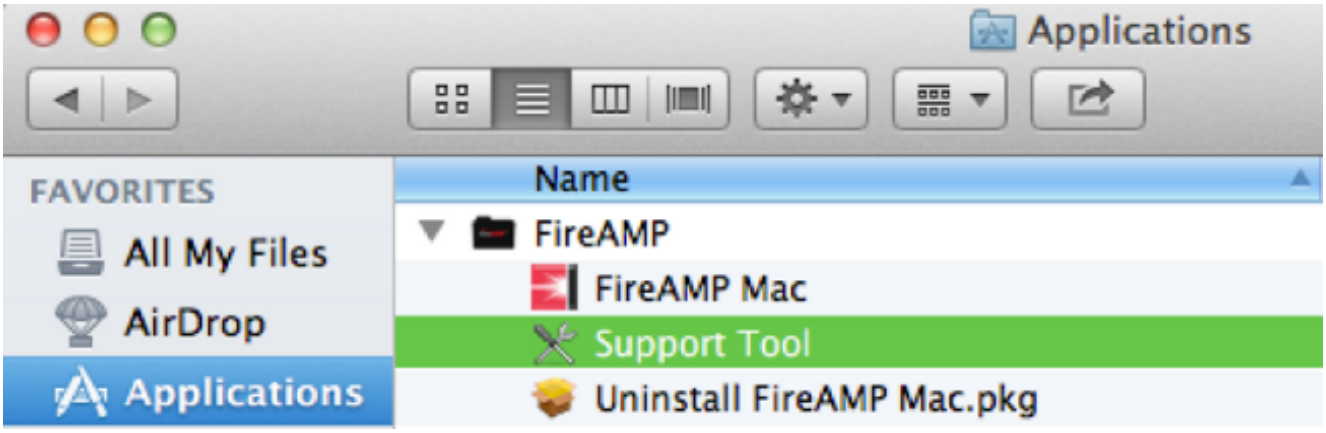
Генерируйте файл диагностики с инструментом поддержки

В этом разделе описывается запустить приложение Инструмента поддержки от GUI или CLI для генерации файла диагностики.

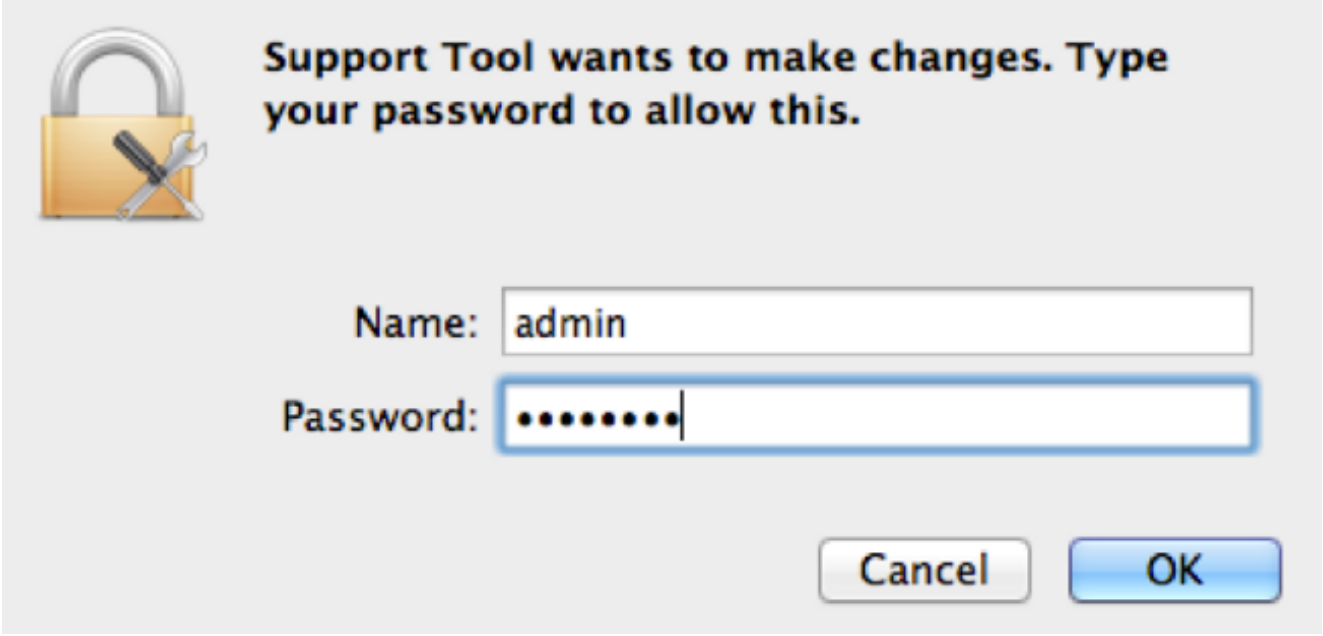
Запустите инструмент поддержки от GUI

Выполните эти шаги для запуска Разъёма FireAMP для Инструмента поддержки Mac от GUI:

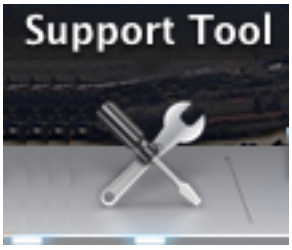
1. Перейдите к каталогу FireAMP в вашей Папке приложений и найдите средство запуска Инструмента поддержки:



2. Дважды нажмите средство запуска Инструмента поддержки, и вам предлагают для административных учетных данных:



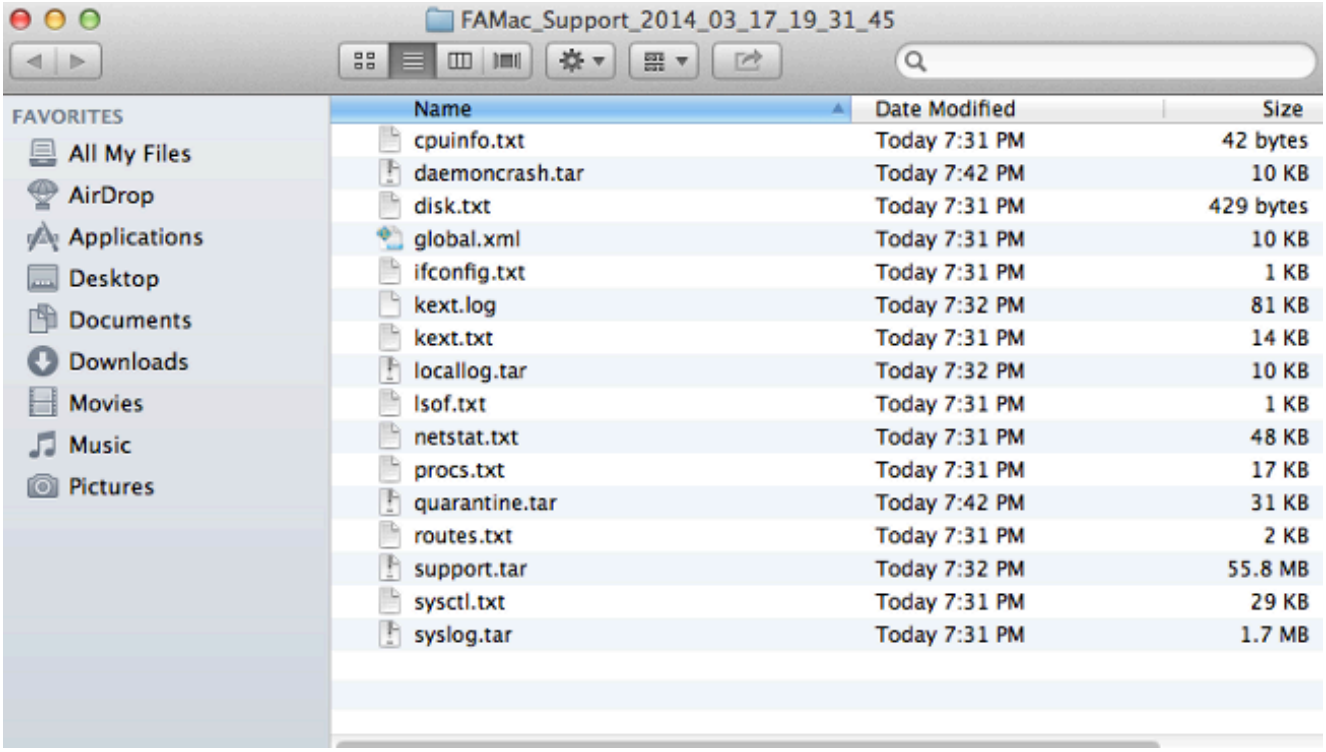
3. После ввода учетных данных значок Инструмента поддержки должен появиться в прикреплении:



Примечание: Выполнение приложения Инструмента поддержки в фоновом режиме и занимает время для завершения (приблизительно 20-30 минут).

4. Когда приложение Инструмента поддержки завершает, файл генерируется и размещается на ваш рабочий стол:

Вот пример разжатых выходных данных:



5. Для анализа данных предоставьте этот файл Команде технической поддержки Cisco.

Запустите инструмент поддержки от CLI

Средство запуска Инструмента поддержки расположено в этом каталоге:

```
/Library/Application Support/Sourcefire/FireAMP Mac/
```

Для запуска приложения Инструмента поддержки введите эту команду в CLI:

> **Примечание:** Необходимо выполнить эту команду как root, поэтому гарантировать, что вы переключаетесь, чтобы базироваться или снабдить команду предисловием с **sudo**.

```
root@mac# cd /Library/Application\ Support/Sourcefire/FireAMP\ Mac
root@mac# ./SupportTool
```

> **Примечание:** Эта команда выполняется многословно. Как только это завершено, файл диагностики генерируется и размещается на ваш рабочий стол.

Устранение неисправностей

В этом разделе описывается включить и отключить режим отладки на Разъёме FireAMP для устранения проблем проблем производительности.

Включите режим отладки

> **% Warning:** Режим отладки должен быть включен, только если Инженер технической поддержки Cisco выполняет запрос для этих данных. Если вы поддерживаете, режим отладки включил для длительного периода времени, он может заполнить дисковое

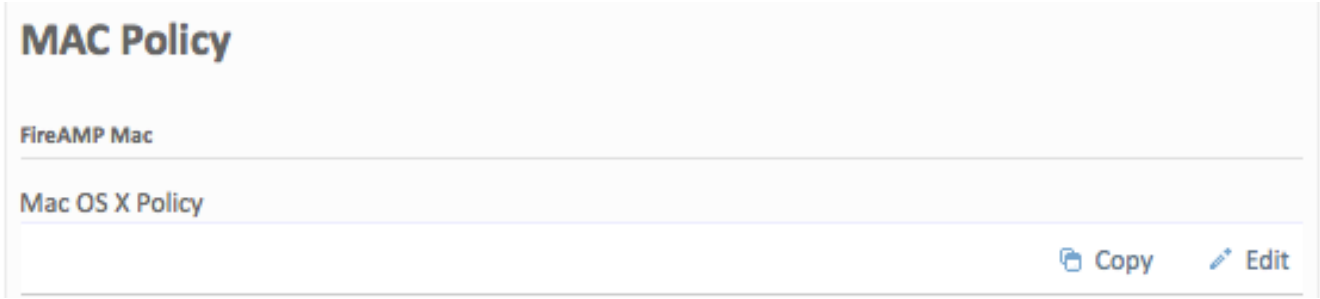
пространство очень быстро и мог бы предотвратить Данные журнала Журнала и Лотка Разъёма от того, чтобы быть собранным в Файле диагностики Поддержки из-за чрезмерного размера файла.

Режим отладки полезен с попытками устранить неполадки проблем производительности на Разъёме FireAMP. Выполните эти шаги, чтобы включить режим отладки и собрать диагностику data:

1. Войдите к облачной консоли FireAMP.

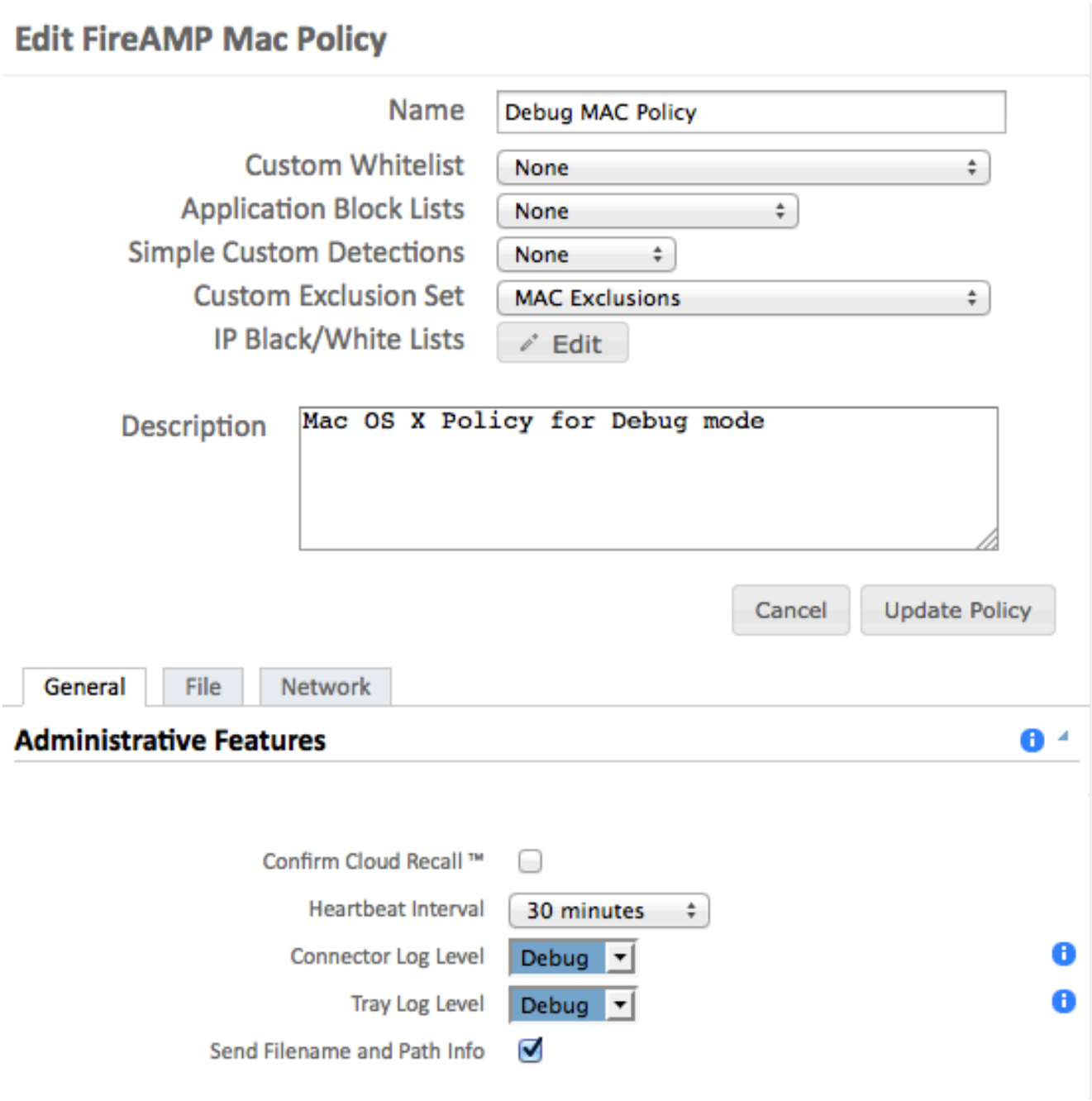
2. Перейдите к **менеджменту> Политика**.

3. Найдите политику, которая применена к компьютеру, и нажмите **Copy**. Консоль FireAMP обновляет со скопированной политикой:



4. Нажмите **Edit** и поменяйте имя политики. Например, вы могли использовать *Политику Debug MAC.*

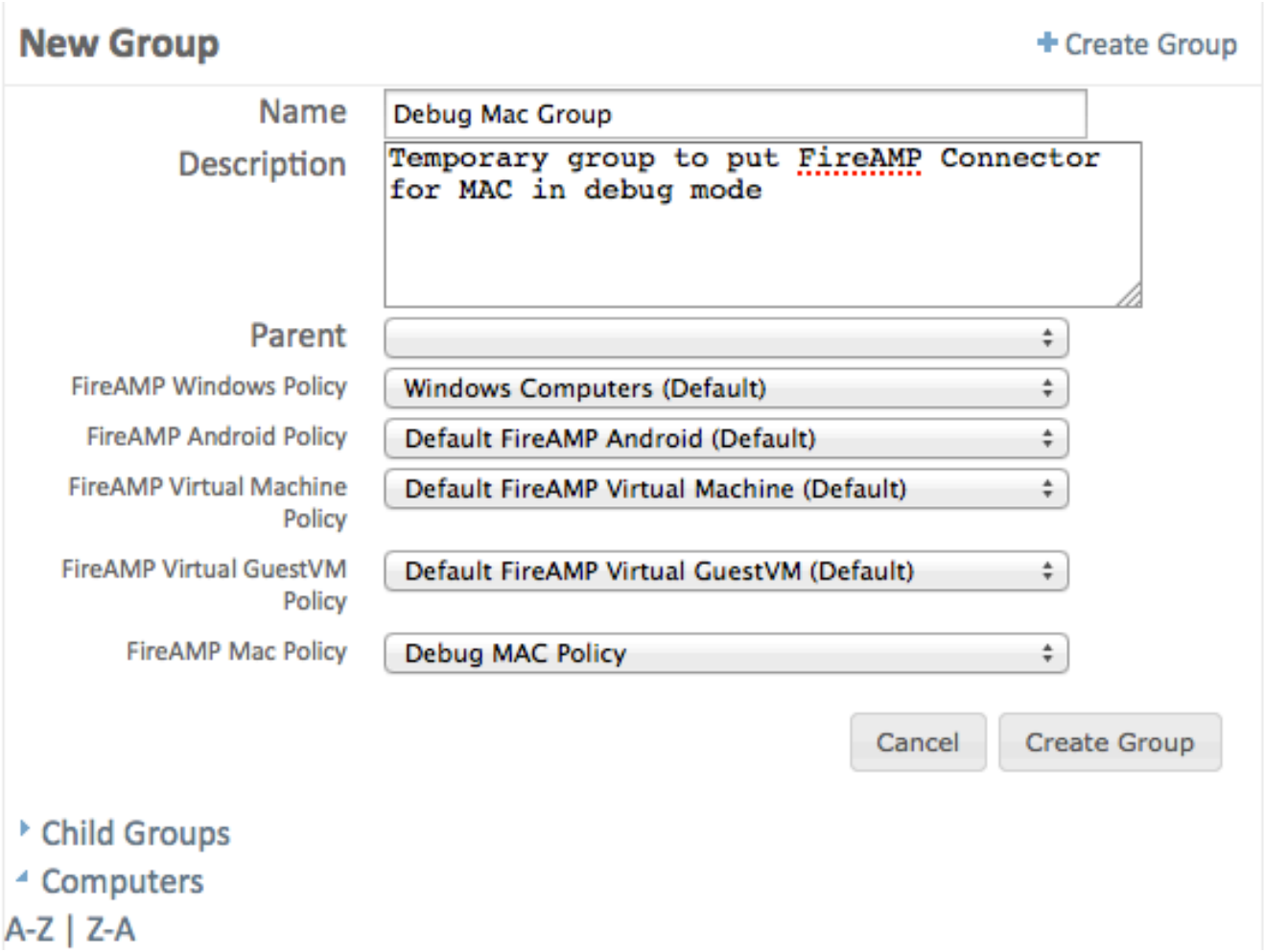
5. Нажмите **Administrative Features** и выберите **Debug** и из выпадающих меню Уровня Журнала Уровня и из Разъёма Журнала Лотка:



6. Нажмите **кнопку Policy Обновления** для сохранения изменений.

7. Перейдите к **менеджменту> Группы** и нажмите **+Create Группу** около верхней правой стороны вашего экрана.

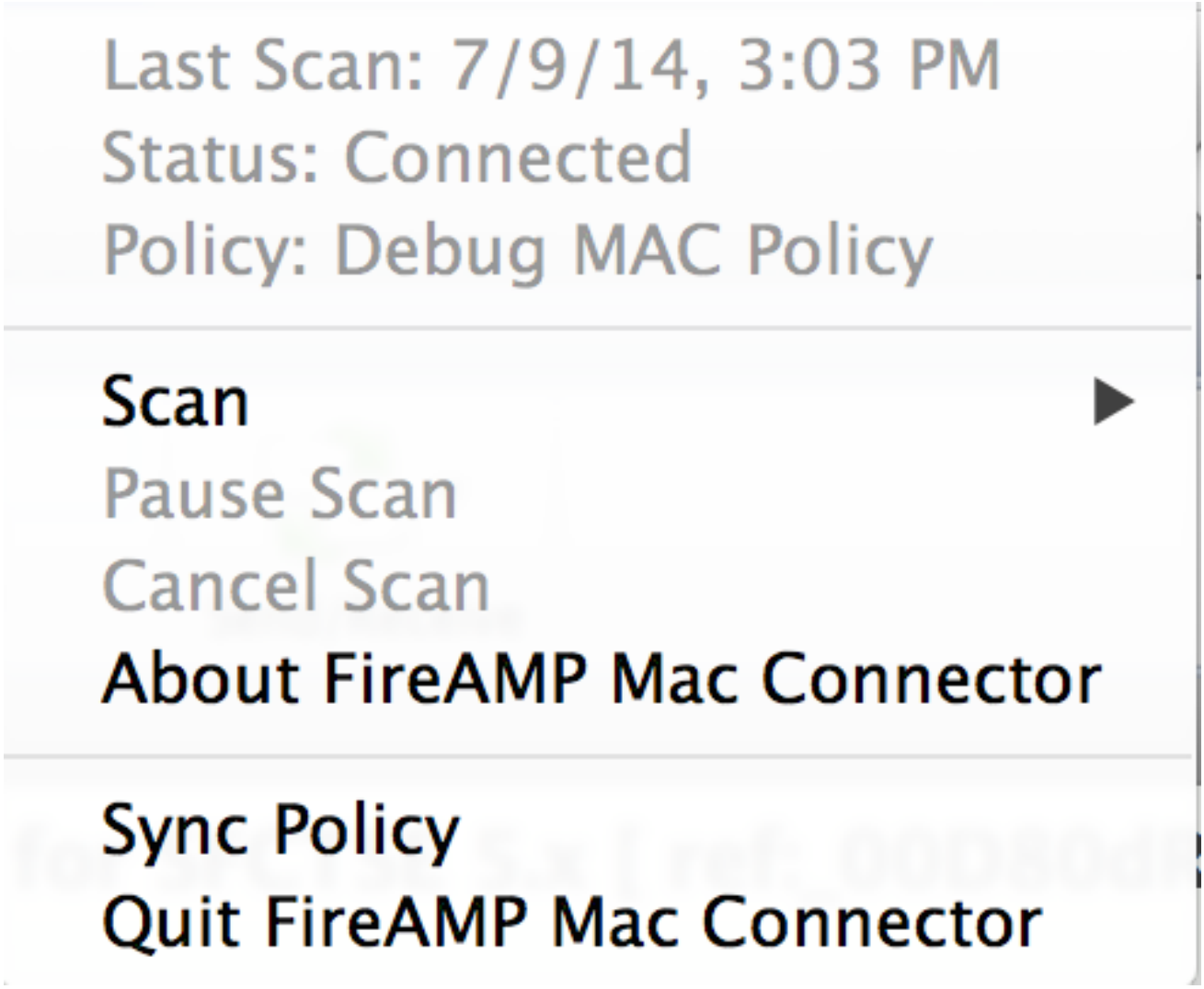
8. Введите имя для группы. Например, вы могли использовать *Debug Mac Group*.



9. Измените политику FireAMP MAC от *Политики Стандартного MAC - адреса* до скопированной, новой политики, которую вы просто создали, который является **Политикой Debug MAC** в данном примере.

10. Нажмите **Computers** и определите свой компьютер в списке. Выберите это и щелчок **добавляет выбранный**.

11. Щелчок **создает группу**. Ваш Mac должен теперь иметь функциональную политику отладки. Можно выбрать значок FireAMP, который появляется на строке меню, и гарантируйте, что применена новая политика:

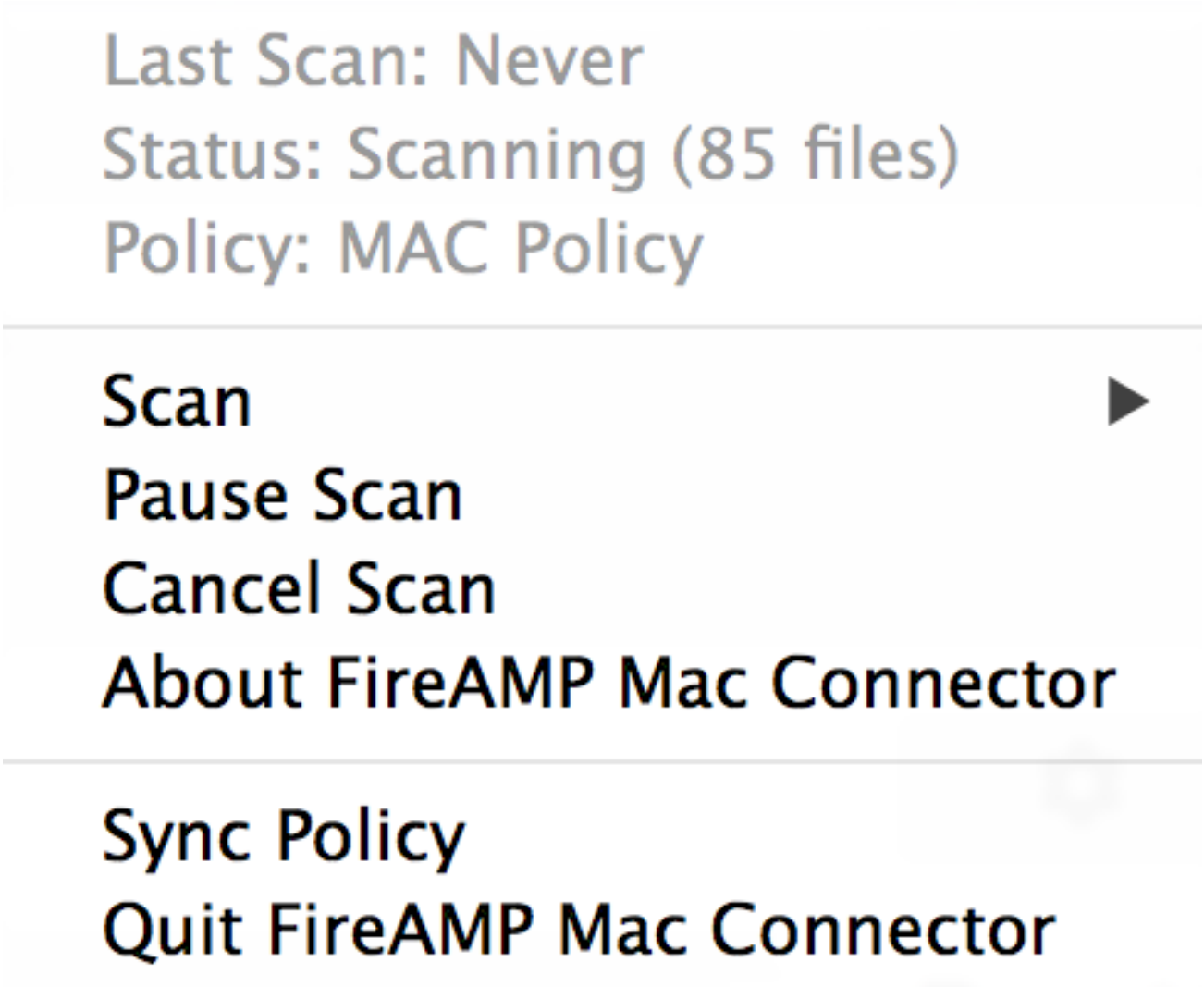


Отключите режим отладки

После диагностических данных в режиме отладки получен, необходимо вернуться Разъём FireAMP назад к обычному режиму. Выполните эти шаги для отключения режима отладки:

1. Войдите к облачной консоли FireAMP.
2. Перейдите к **менеджменту> Группы**.
3. Найдите новую группу, *Debug MAC Group*, которую вы создали в режиме отладки.
4. **Нажмите Edit.**
5. Нажмите **Computers** и найдите свой компьютер в списке. Выберите это и щелчок **удаляет выбранный**.
6. Нажмите **группу обновления**.
7. Нажмите **Sync Policy** на строке меню, где расположен значок FireAMP.
8. Проверьте, что политика теперь возвращена к предыдущему значению по умолчанию. Проверьте это на строке меню. Политика должна была теперь вернуться назад к

исходной политике, которая использовалась перед изменением его на *Политику Debug MAC*:



Режим отладки теперь отключен, и Разъём FireAMP должен обычно функционировать.