FireAMP Connector for Mac Diagnostic Data Collection

Document ID: 118365

Contributed by Nazmul Rajib, Justin Roberts, and Nikhil Vaidya, Cisco TAC Engineers.
Mar 11, 2015

Contents

Introduction

This document describes the process that is used in order to generate a diagnostic file via the Support Tool application that is available on the Cisco FireAMP Connector for Macintosh (Mac) machines and how to troubleshoot performance issues.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco FireAMP Connector for Mac
- Mac OSX

Components Used

The information in this document is based on the Cisco FireAMP Connector for Mac.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Background Information

The Cisco FireAMP Connector for Mac installs an application called *Support Tool*, which is used in order to generate diagnostic information about the FireAMP Connector that is installed on your Mac. The diagnostic

data includes information about your Mac such as:

- Resource utilization (disk, CPU, and memory)
- FireAMP−specific logs
- FireAMP configuration information

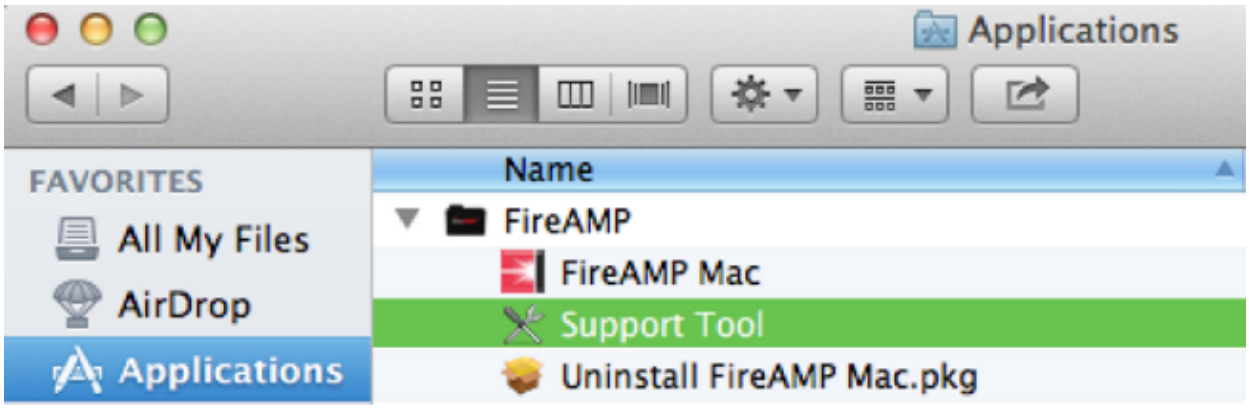
Generate a Diagnostic File with the Support Tool

This section describes how to launch the Support Tool application from the GUI or the CLI in order to generate a diagnostic file.

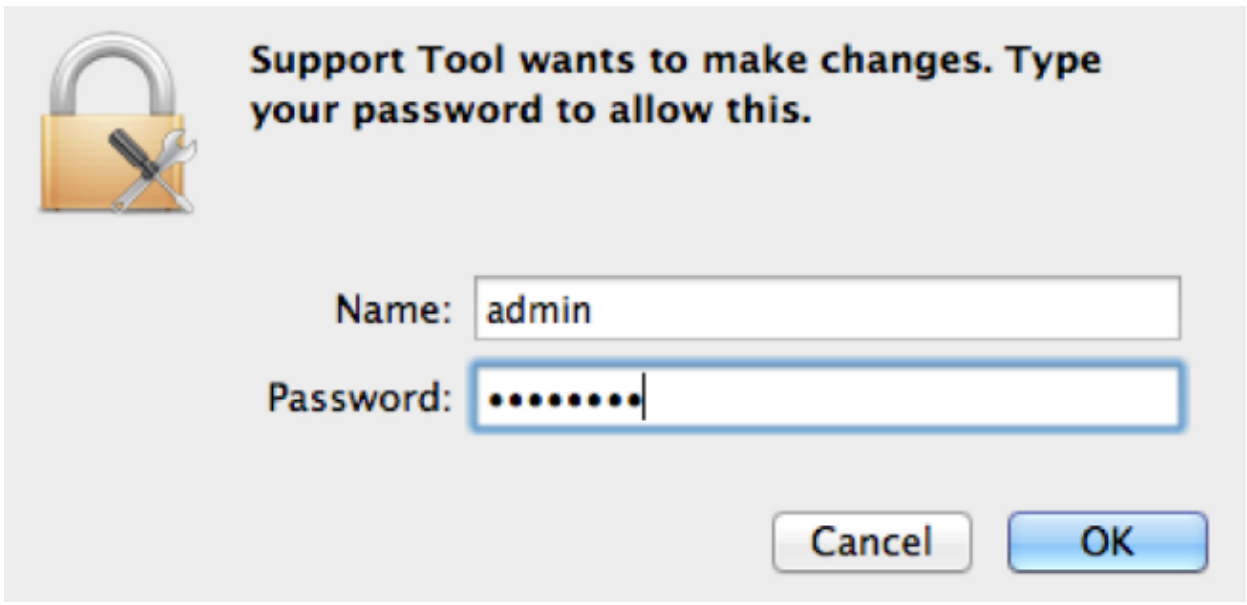
Launch the Support Tool from the GUI

Complete these steps in order to launch the FireAMP Connector for Mac Support Tool from the GUI:

1. Navigate to the FireAMP directory in your Applications folder and locate the Support Tool launcher:



2. Double−click the Support Tool launcher, and you are prompted for administrative credentials:

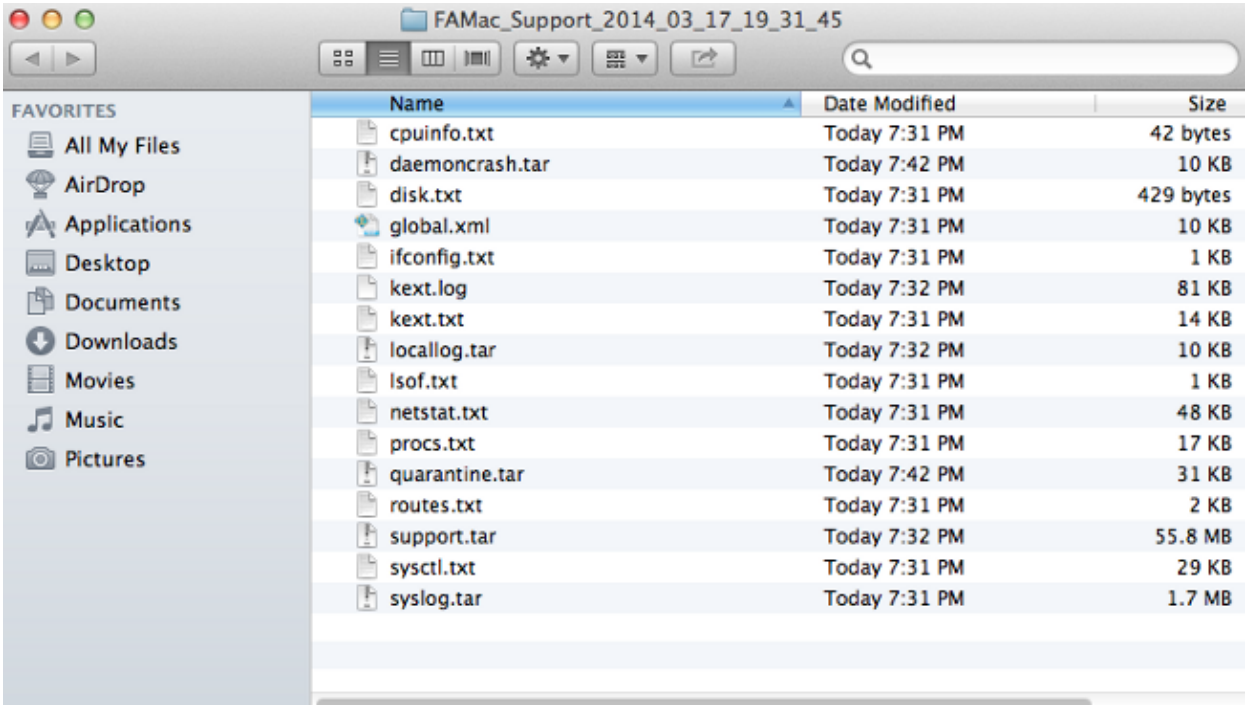


3. After you enter your credentials, the Support Tool icon should appear in your dock:

Note: The Support Tool application runs in the background and takes some time to complete (approximately 20−30 minutes).

4. When the Support Tool application completes, a file is generated and placed onto your desktop:

Here is an example of the uncompressed output:



5. In order to analyze the data, provide this file to the Cisco Technical Support Team.

Launch the Support Tool from the CLI

The Support Tool launcher is located in this directory:

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

In order to launch the Support Tool application, enter this command into the CLI:

Note: You must run this command as root, so ensure that you switch to root or preface the command with ***sudo***.

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

```
root@mac# ./SupportTool
```

Note: This command runs verbosely. Once it is complete, a diagnostic file is generated and placed onto your desktop.

Troubleshooting

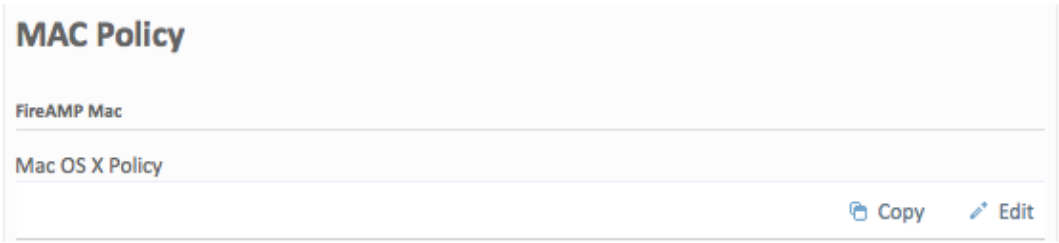
This section describes how to enable and disable debug mode on the FireAMP Connector in order to troubleshoot performance issues.

Enable Debug Mode

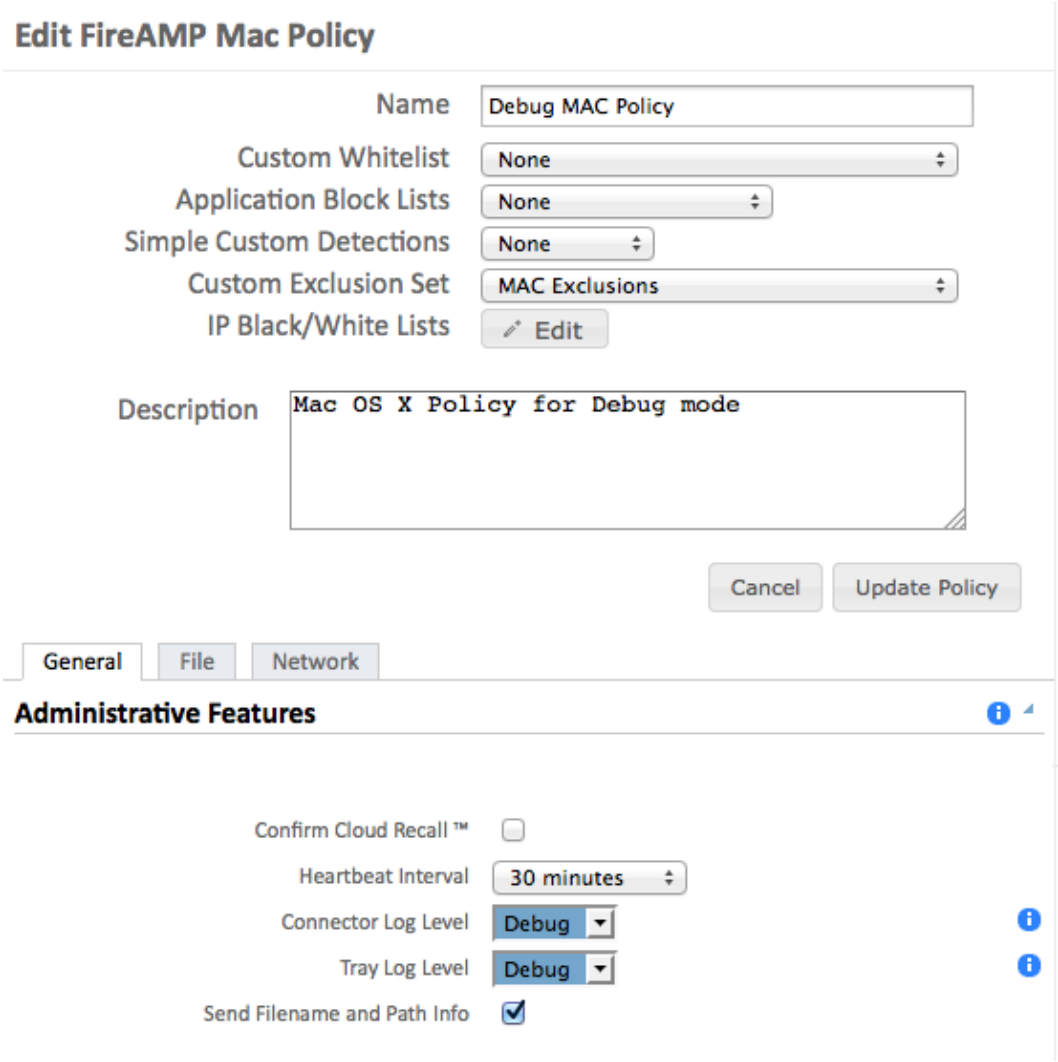
Warning: Debug mode should be enabled only if a Cisco Technical Support Engineer makes a request for this data. If you keep debug mode enabled for an extended period of time, it can fill up the disk space very quickly and might prevent the Connector Log and Tray Log data from being gathered in the Support Diagnostic file due to excessive file size.

Debug mode is useful with attempts to troubleshoot performance issues on a FireAMP Connector. Complete these steps in order to enable debug mode and collect diagnostic data:

1. Log in to the FireAMP Cloud Console.
2. Navigate to ***Management*** > ***Policies***.
3. Locate a policy that is applied to a computer and click ***Copy***. The FireAMP Console updates with the copied policy:



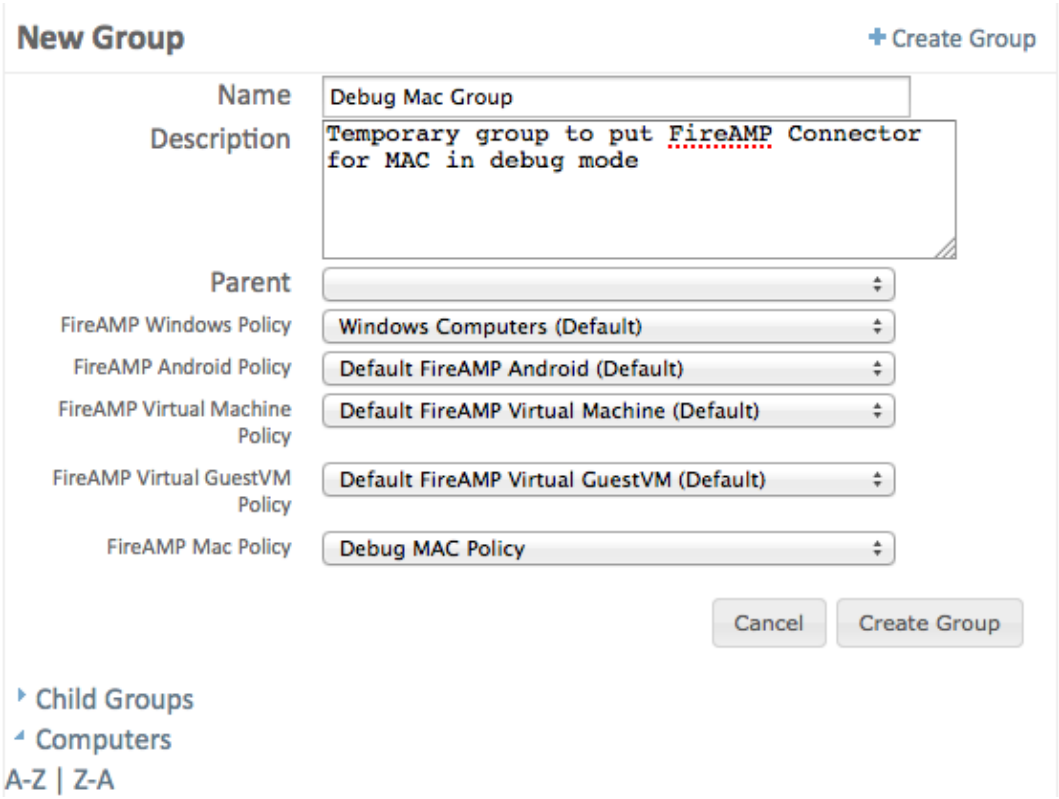
4. Click ***Edit*** and change the name of the policy. For example, you could use *Debug MAC Policy*.
5. Click ***Administrative Features*** and select ***Debug*** from both the Tray Log Level and Connector Log Level drop down menus:



6. Click the ***Update Policy*** button in order to save the changes.

7. Navigate to ***Management*** > ***Groups*** and click ***+Create Group*** near the top−right side of your screen.

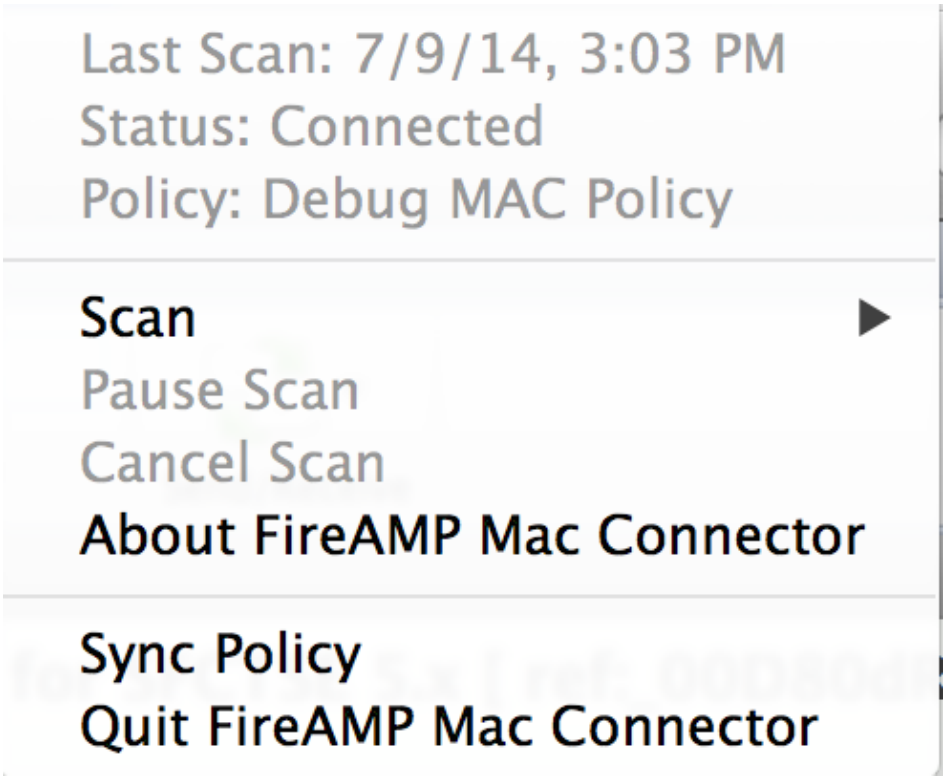
8. Enter a name for the group. For example, you could use *Debug Mac Group*.



9. Change the FireAMP MAC Policy from *Default MAC Policy* to the copied, new policy that you just created, which is ***Debug MAC Policy*** in this example.

10. Click ***Computers*** and identify your computer in the list. Select it and click ***add selected***.

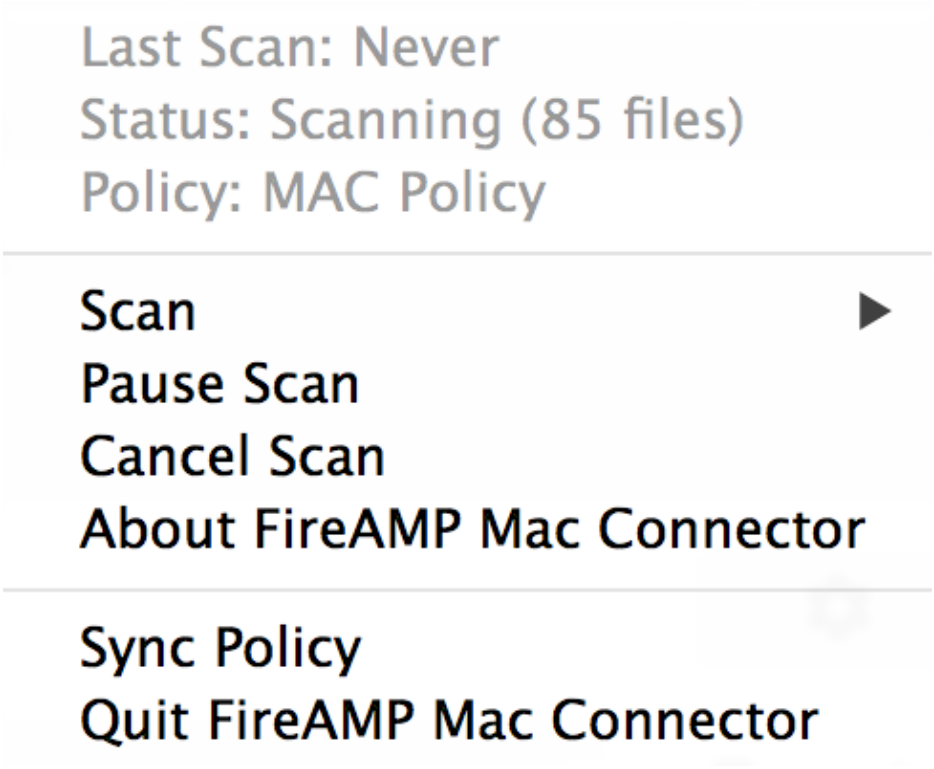
11. Click ***create group***. Your Mac should now have a functional debug policy. You can select the FireAMP icon that appears on your menu bar and ensure that the new policy is applied:



Disable Debug Mode

After the diagnostic data in debug mode is obtained, you must revert the FireAMP Connector back to the normal mode. Complete these steps in order to disable debug mode:

1. Log in to the FireAMP Cloud Console.
2. Navigate to ***Management > Groups***.
3. Locate the new group, *Debug MAC Group*, that you created in debug mode.
4. Click ***Edit***.
5. Click ***Computers*** and locate your computer in the list. Select it and click ***remove selected***.
6. Click ***update group***.
7. Click ***Sync Policy*** on the menu bar where the FireAMP icon is located.
8. Verify that the policy is now returned to the previous default value. Check this on the menu bar. The policy should now have reverted back to the original policy that was used before you changed it to the *Debug MAC Policy*:



Debug mode is now disabled, and the FireAMP Connector should function normally.

Updated: Mar 11, 2015 Document ID: 118365