Collection of Diagnostic Data from a FireAMP Connector Running on Windows

Contents

Introduction

This document describes the steps to generate a diagnostic file from a FireAMP Connector. If you experience a technical issue with a FireAMP connector that runs on Microsoft Windows, a Cisco Technical Support Engineer might want to analyze the log messages available in a diagnostic file.

Generate Diagnostic File

Dependent upon the version of Windows, navigation to the Support Diagnostic Tool of FireAMP Connector might be different. In most Windows operating systems, you go to the Start menu in order to find the Support Diagnostic Tool of FireAMP Connector. For example:

Start > **All Programs** > **FireAMP Connector** > **Support Diagnostic Tool**.

> **Note**: If you run Windows with the User Account Control, click **Yes** in order to allow the tool to run.

The Support Diagnostic Tool creates a compressed file in 7z format and saves it on the Desktop. Here is an example of the filename of a diagnostic file on a Desktop:

v5.0 and earlier: `Sourcefire_Support_Tool_YYYY_MM_DD_HH_MM_SS.7z`

v5.1 and newer: `CiscoAMP_Support_Tool_YYYY_MM_DD_HH_MM_SS.7z`

Alternatively, you can run this executable file as an administrator:

```
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
```

Debug Mode

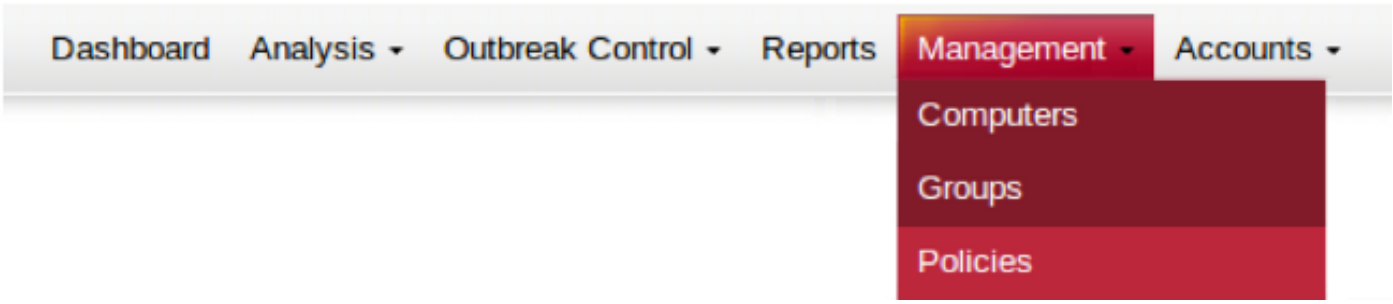
Enablement of debug mode on a FireAMP connector provides additional verbosity to the logging, which allows more insight into problems with connector. This section describes how to enable debug mode in a FireAMP connector.

Warning: Debug mode should be enabled only if a Cisco Technical Support Engineer requests this data. Enabling debug mode for a longer time can fill up the disk space very quickly and might prevent the Support Diagnostic file from gathering the **Connector Log** and **Tray Log** due to excessive file size.

Enable Debug Mode

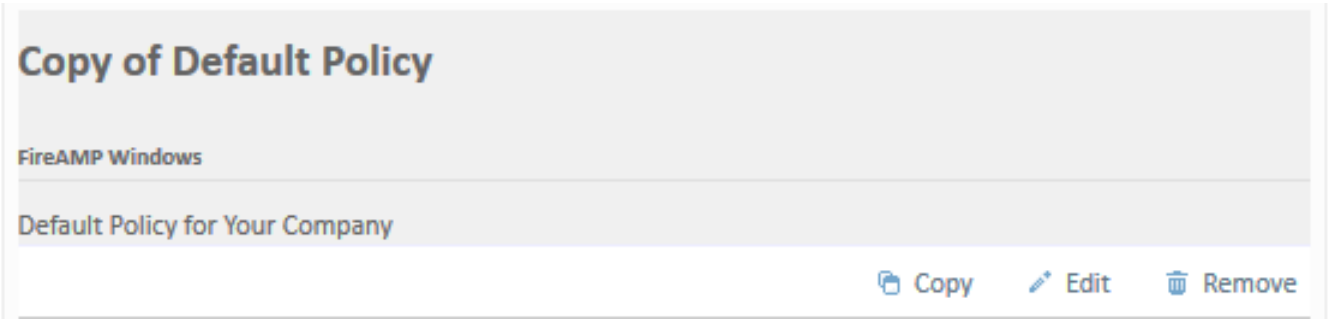
Step 1: Log into the FireAMP console.

Step 2: Choose **Managment > Policies**.

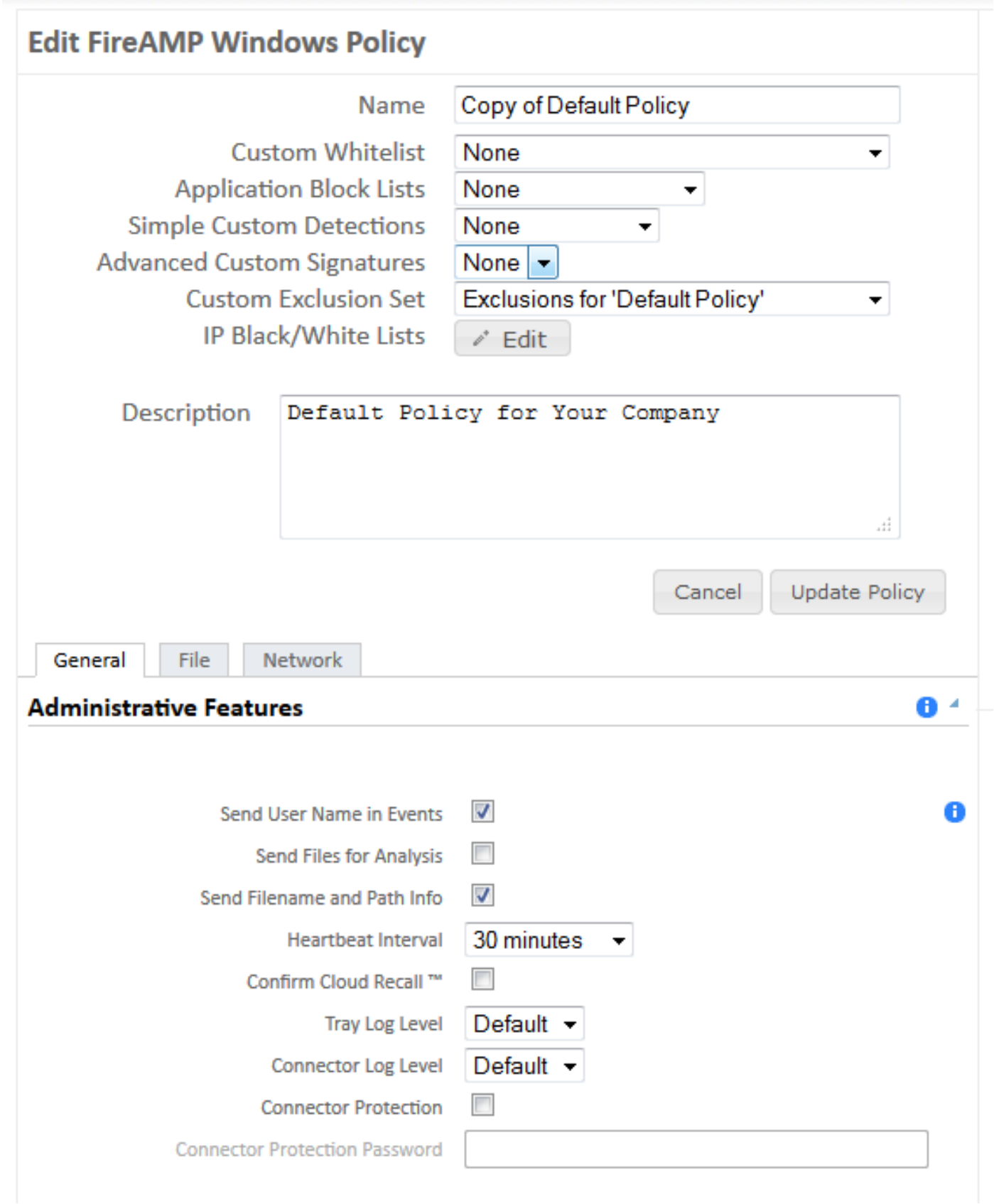


Step 3: Locate the Policy that is applied to the end device or computer and click **Copy.**

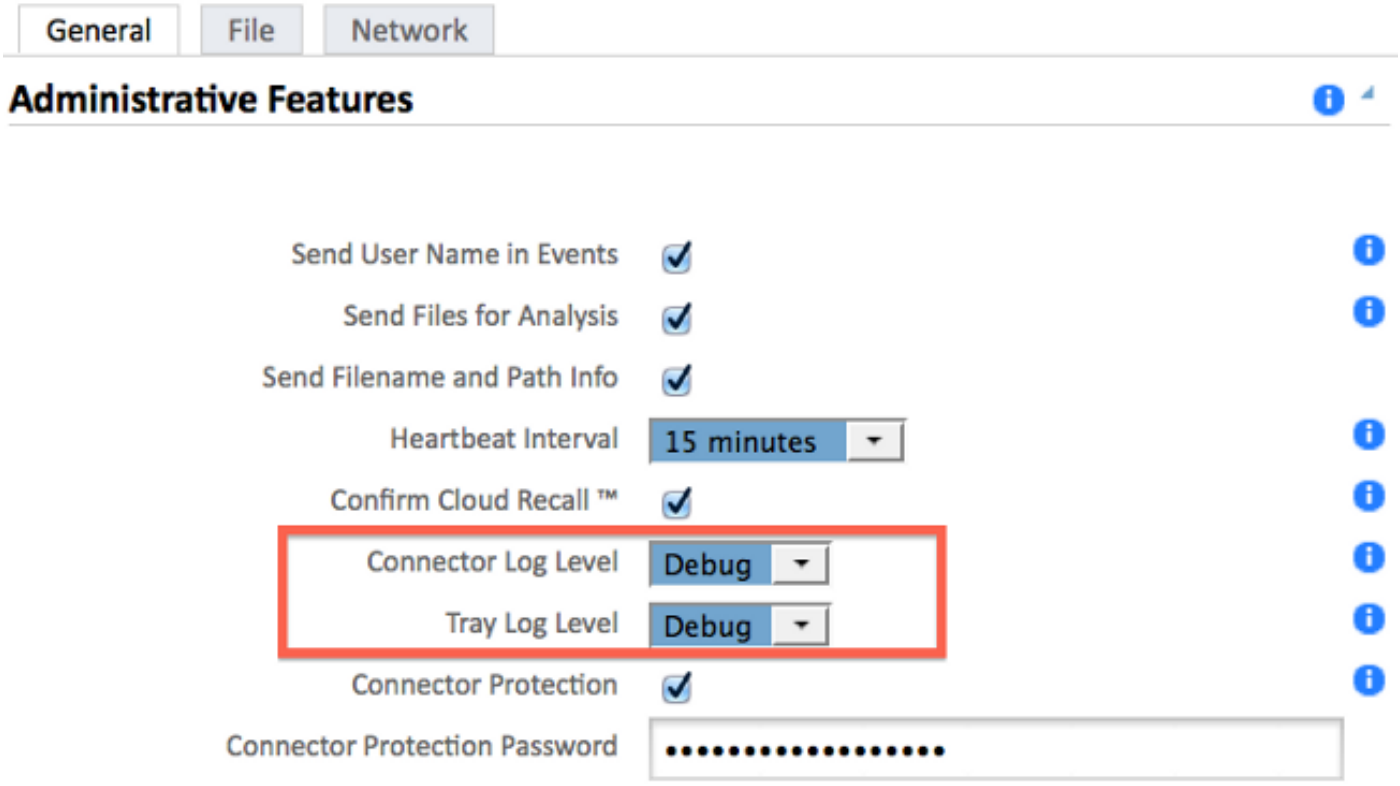
Step 4: After you click Copy, the FireAMP Console updates with the copied policy.



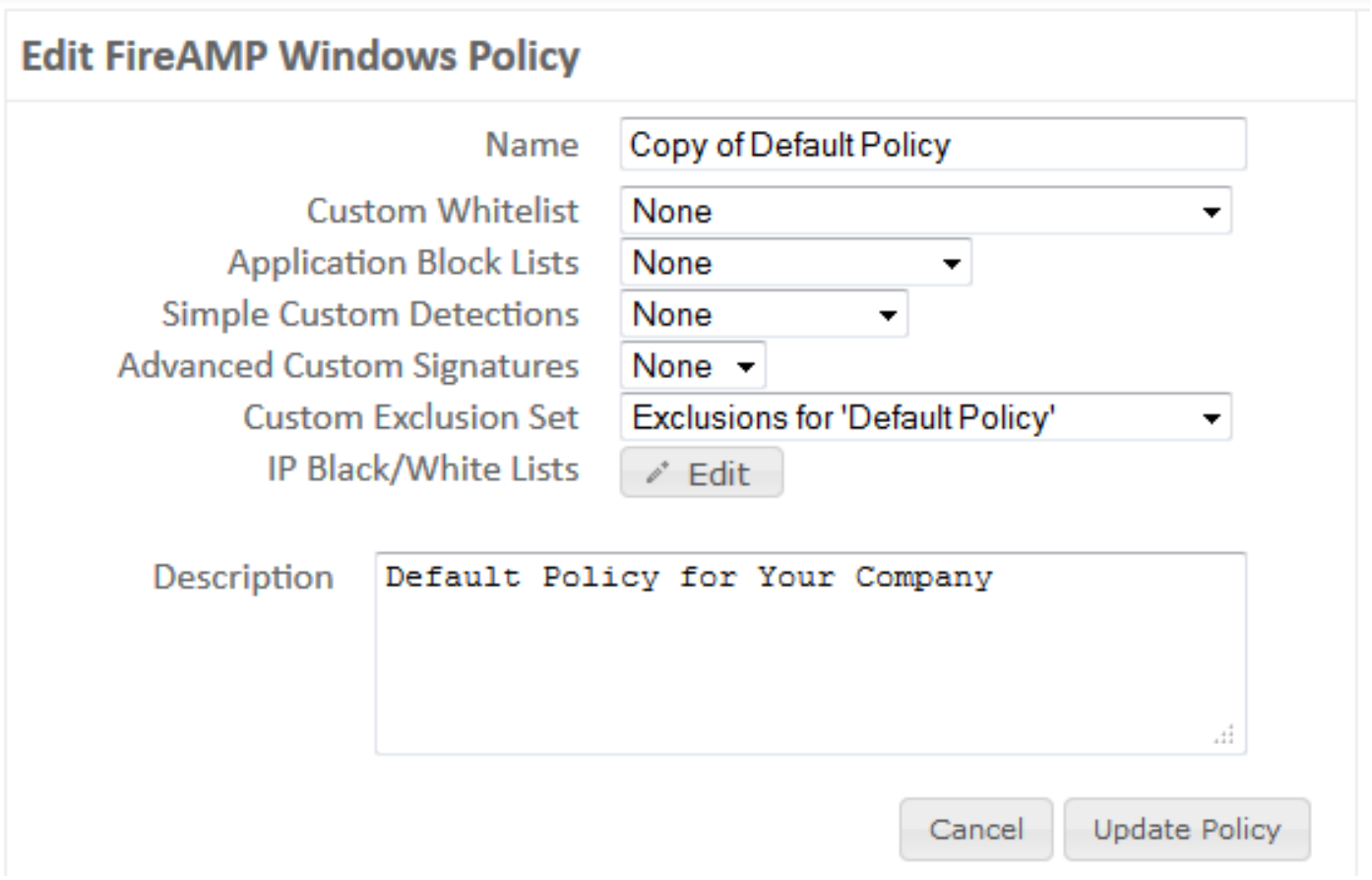
Step 5:Click **Edit** and then click **Administrative Features**.



Step 6: For **Tray Log Level** and **Connector Log Level**, choose **Debug** from the drop-down lists.



Step 7: Click **Update Policy** in order to save the changes.

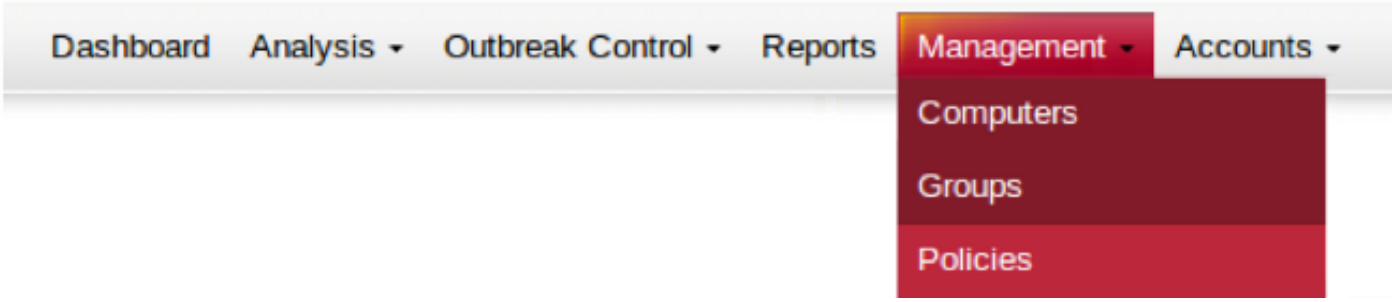


Step 8: After you update the policy, you need to apply this on the end device where you want to generate debug information.

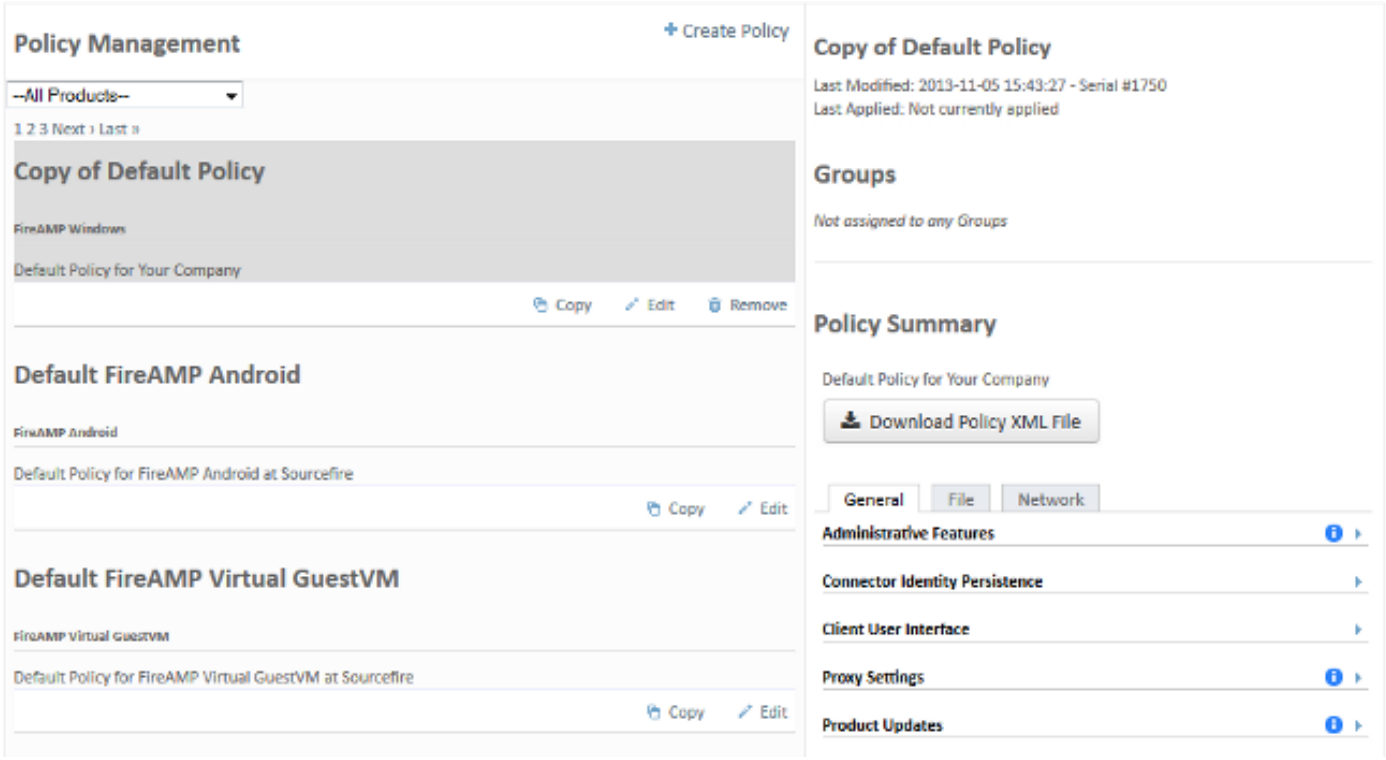
Unable to Enable Debug Mode

Due to the connectivity issue, if you are unable to apply policy to a FireAMP Connector you will be unable to enable the debug mode. In that case, you can download the `policy.xml` file and configure the FireAMP Connector to use your modified policy. Follow these instructions if the FireAMP cloud is unable to communicate with the FireAMP connector:

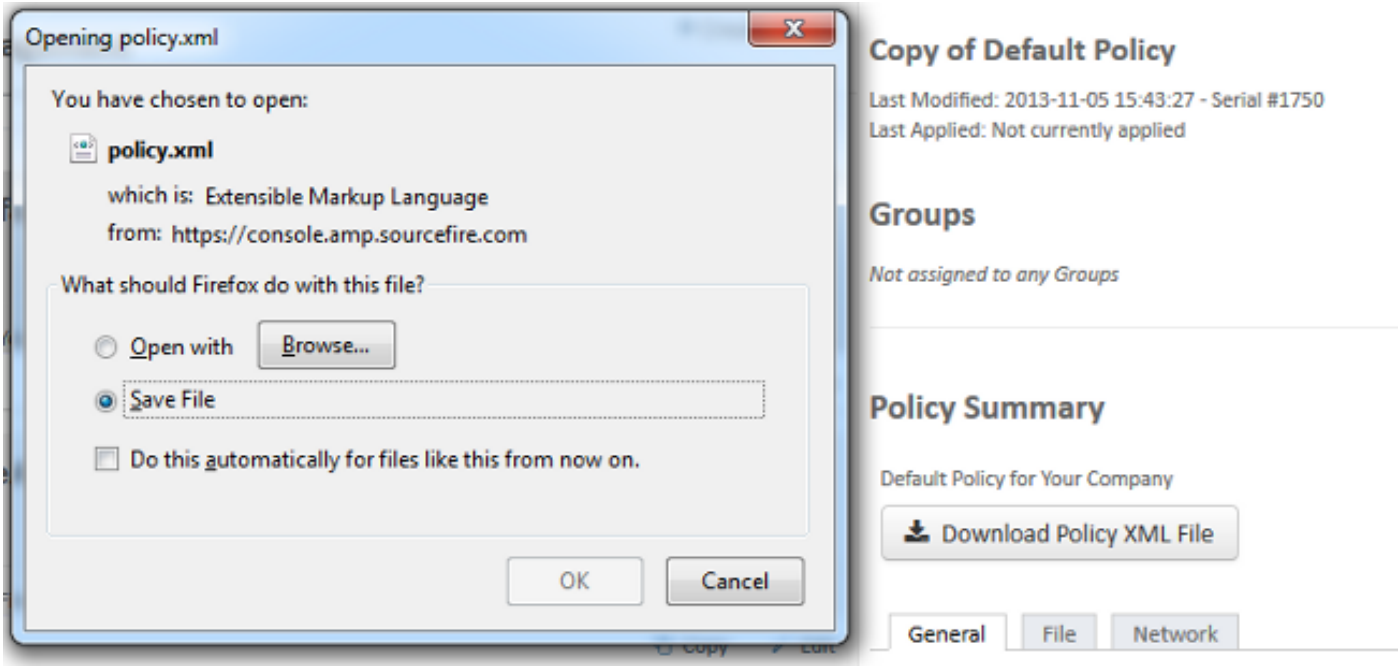
Step 1: Choose **Management > Policies**.



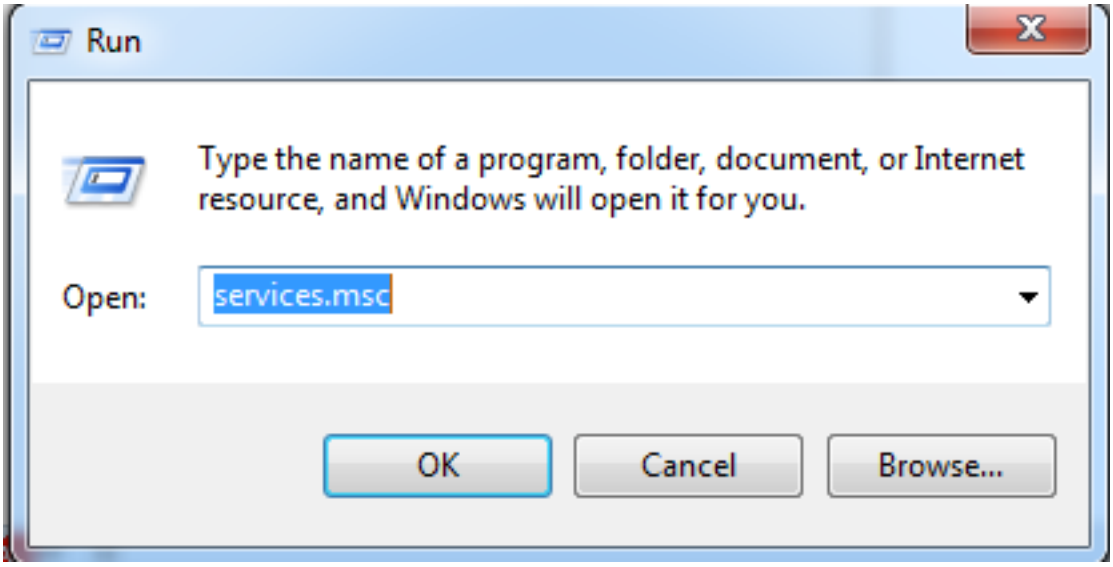
Step 2: Locate the Policy that was copied and click on the name in order to display the **Policy Summary**.



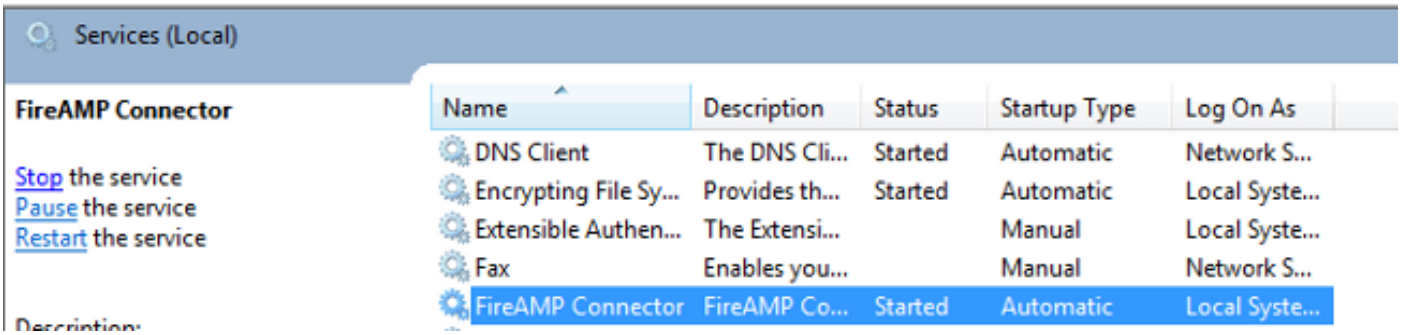
Step 3: Click **Download Policy XML File** and then save the file to your computer.



Step 4: Open **`services.msc`** with **Start > Run**.



Step 5: Locate the **FireAMP Connector** service and click **Stop**.



Step 6: Click **Start > Computer**, then navigate to one of these directories depending on the computer architecture:

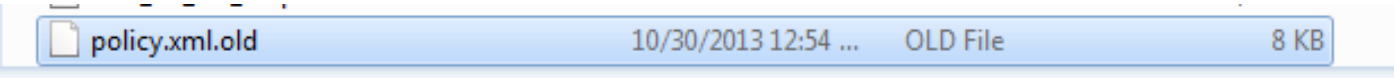
In x86 Platform:

```
v5.0 and earlier: C:\Program Files (x86)\Sourcefire\fireAMP
v5.1 and newer: C:\Program Files (x86)\Cisco\AMP
```

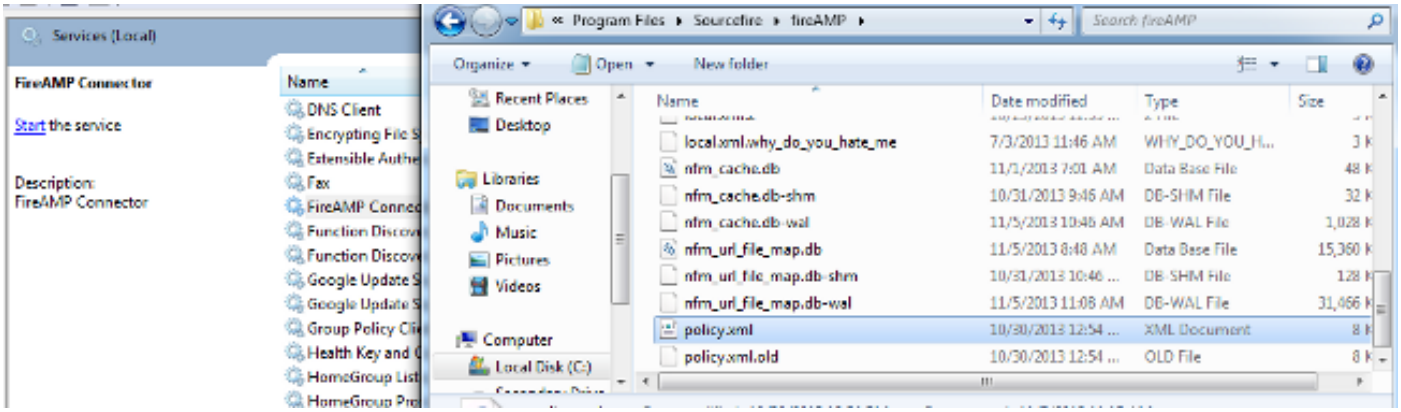
In x64 Platform:

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

Step 7: Locate the file `policy.xml, and rename the file to policy.xml.old.`



Step 8: Move the downloaded `policy.xml` into the directory and then click **Start the service** in the Services window. The FireAMP Connector is now in debug mode and logs additional diagnostic data.



In order to disable debug mode, perform Step 5 through Step 8, undo the changes to `policy.xml.old, and restart the FireAMP Connector.`