

Índice

[Introdução](#)

[Gere o arquivo de diagnóstico](#)

[Debugar o modo](#)

[Permita debugar o modo](#)

[Incapaz de permitir debugar o modo](#)

Introdução

Este documento descreve as etapas para gerar um arquivo de diagnóstico de um conector de FireAMP. Se você experimenta uma questão técnica com um conector de FireAMP que fosse executado em Microsoft Windows, um engenheiro de suporte técnico de Cisco pôde querer analisar os mensagens de registro disponíveis em um arquivo de diagnóstico.

Gere o arquivo de diagnóstico

O dependente em cima da versão de janela, navegação à ferramenta de diagnóstico do apoio do conector de FireAMP pôde ser diferente. Na maioria de sistemas operacionais de Windows, você vai ao menu de início a fim encontrar a ferramenta de diagnóstico do apoio do conector de FireAMP. Por exemplo:

Começo > todos os programas > conector de FireAMP > ferramenta de diagnóstico do apoio.

Nota: Se você executa Windows com o controle da conta de usuário, clique **sim** a fim permitir que a ferramenta seja executado.

A ferramenta de diagnóstico do apoio cria um arquivo compactado no formato 7z e salvar o no Desktop. Está aqui um exemplo do nome de arquivo de um arquivo de diagnóstico em um Desktop:

`Sourcefire_Support_Tool_2016_01_15_10_44_11.7z`

Alternativamente, você pode executar este arquivo executável como um administrador:

`C:\Program Files\Sourcefire\fireAMP\X.X.X\ipsupporttool.exe`

Debugar o modo

A habilitação de debugar o modo em um conector de FireAMP fornece a verbosidade adicional ao registro, que reserva mais introspecção em problemas com conector. Esta seção descreve como permitir debugar o modo em um conector de FireAMP.

aviso: Debugar o modo deve ser permitido somente se um engenheiro de suporte técnico de Cisco pede estes dados. Permitir debugar o modo por um tempo mais longo pode encher

acima o espaço de disco muito rapidamente e pôde impedir que o arquivo de diagnóstico do apoio recolha o **log do conector** e o **log da bandeja** devido ao tamanho do arquivo excessivo.

Depois que você roda a ferramenta de diagnóstico do apoio debugar o modo, os dados adicionais está armazenado nestes arquivos:

- sfc.exe.log
- iptray.exe.log

Estes arquivos são armazenados no dobrador do fireAMP situado sob o diretório de arquivos de programa. Neste exemplo, 3.x.x é a versão do conector de FireAMP instalado no host.

Nas Plataformas x86:

C:\Program Files\Sourcefire\fireAMP\X.X.X\ipsupporttool.exe

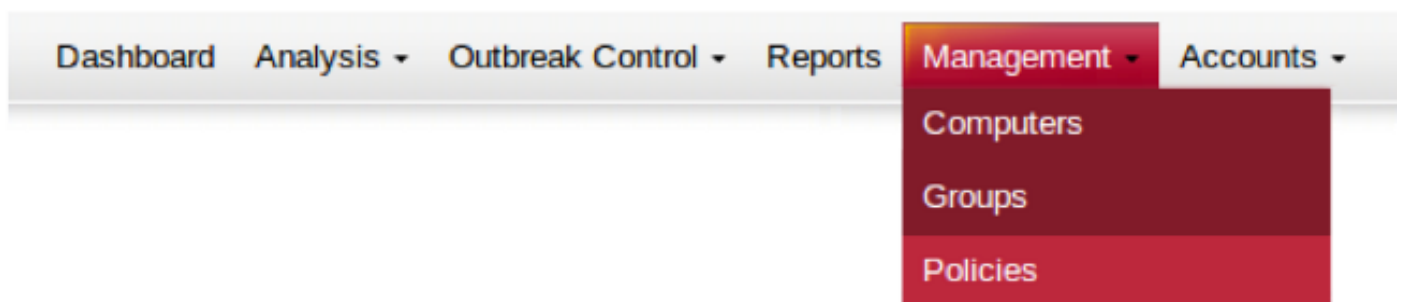
Nas Plataformas x64:

C:\Program Files\Sourcefire\fireAMP\X.X.X\ipsupporttool.exe

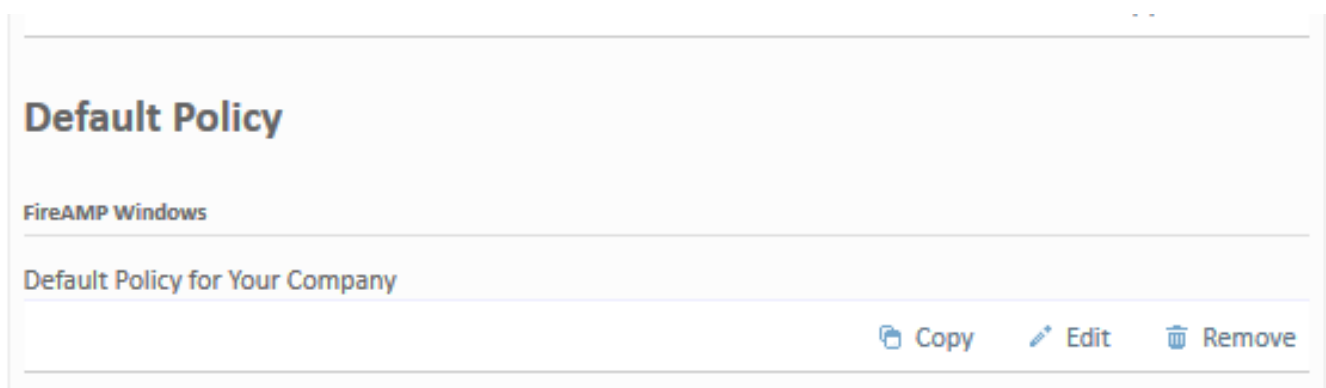
Permita debugam o modo

Passo 1: Log no console de FireAMP.

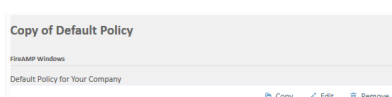
Passo 2: Escolha o **Gerenciamento > as políticas**.



Passo 3: Encontre a política que é aplicada ao dispositivo final ou ao computador e clique a **cópia**.



Passo 4: Depois que você clica a cópia, as atualizações do console de FireAMP com a política copiada.



A etapa 5: Click **edita** e clica então **características administrativas**.

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"/>

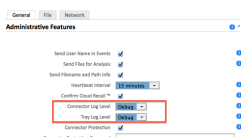
Description

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"/>

Passo 6: Para o nível do log da bandeja e o nível do log do conector, escolha **debug** das listas de drop-down.



Passo 7: Política da atualização do clique a fim salvar as mudanças.

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

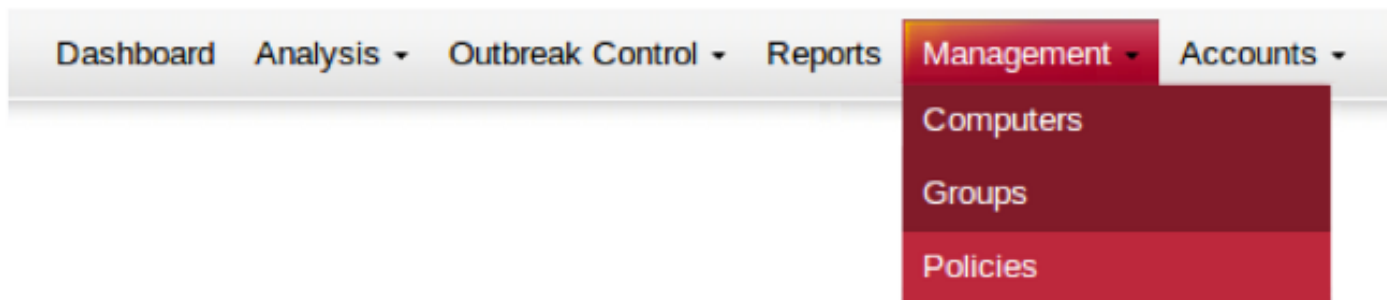
Buttons: Cancel, Update Policy

Passo 8: Depois que você atualiza a política, você precisa de aplicar este no dispositivo final onde você quer gerar debug a informação.

Incapaz de permitir debugar o modo

Devido ao problema de conectividade, se você é incapaz de aplicar a política a um conector de FireAMP você será incapaz de permitir o modo debugar. Nesse caso, você pode transferir o arquivo `policy.xml` e configurar o conector de FireAMP para usar sua política alterada. Siga estas instruções se a nuvem de FireAMP é incapaz de se comunicar com o conector de FireAMP:

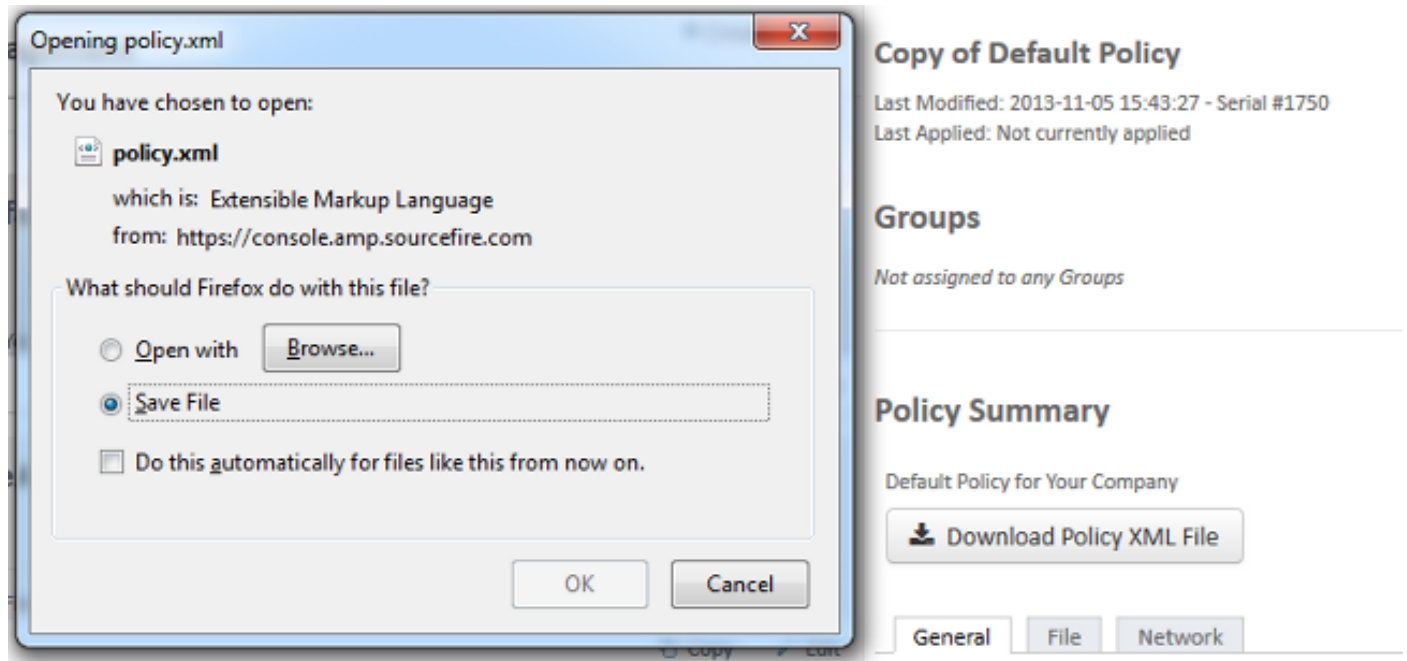
Passo 1: Escolha o **Gerenciamento > as políticas**.



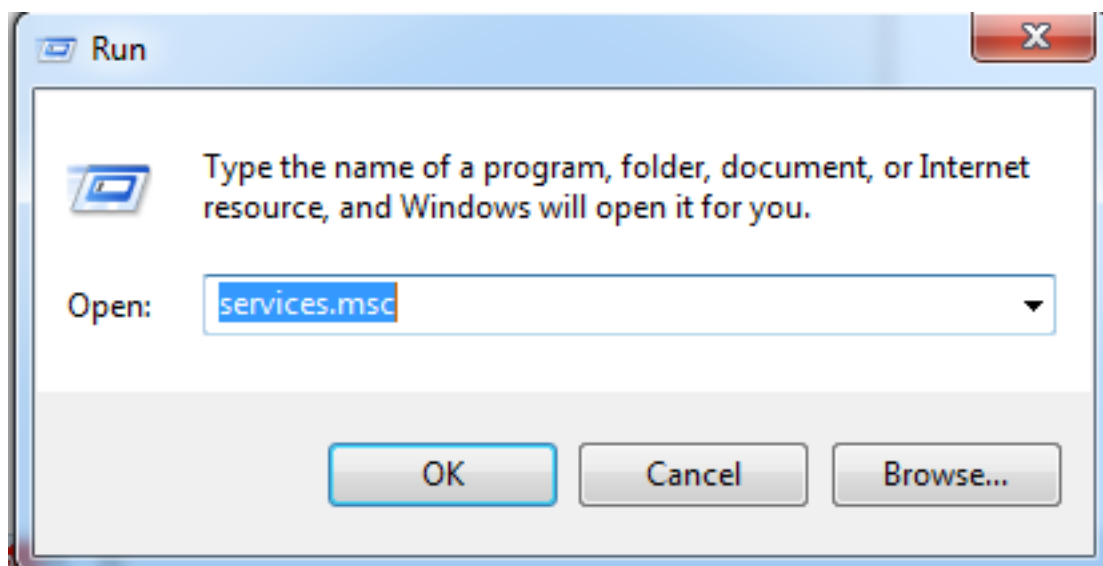
Passo 2: Encontre a política que foi copiada e clique sobre o nome a fim indicar o **sumário da política**.



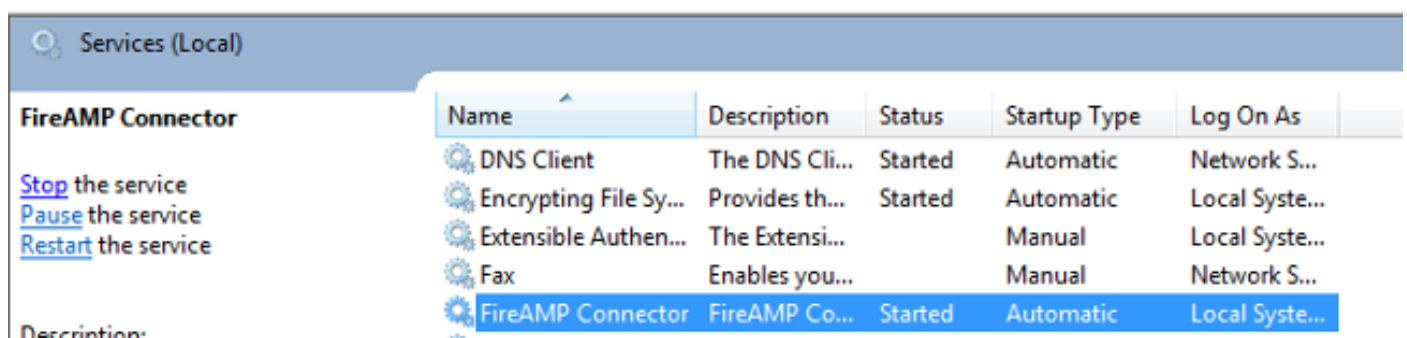
Passo 3: Clique o **arquivo da política XML da transferência** e salvar então o arquivo a seu computador.



Passo 4: Abra **services.msc** com Iniciar > Executar.



Passo 5: Encontre o serviço do **conector de FireAMP** e clique a **parada**.



Passo 6: Clique o **começo** > **o computador**, a seguir navegue a um destes diretórios segundo a arquitetura informática:

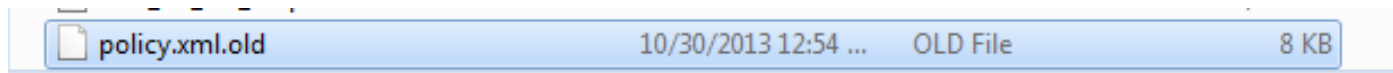
Na plataforma x86:

C:\Program Files\Sourcefire\fireAMP\X.X.X\ipsupporttool.exe

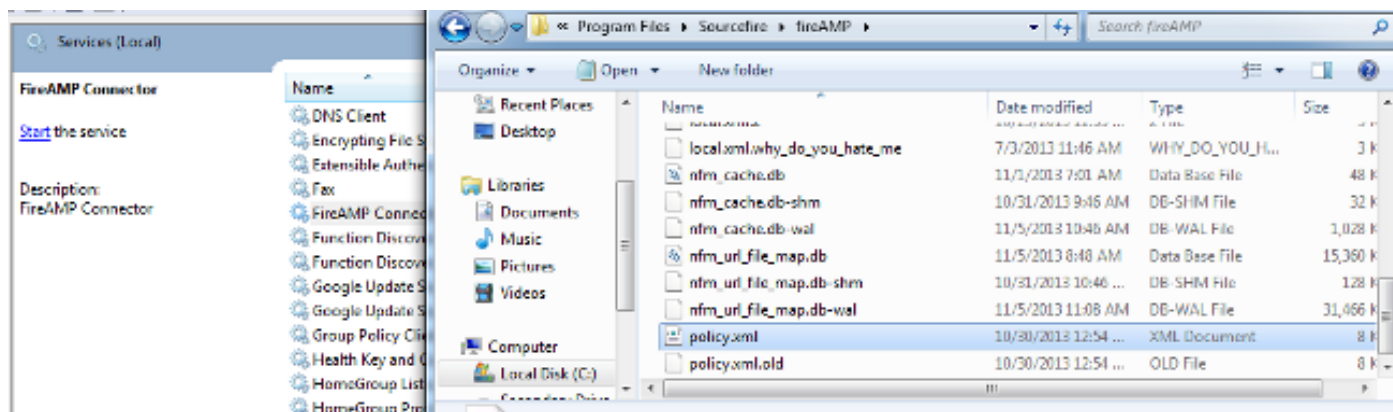
Na plataforma x64:

C:\Program Files\Sourcefire\fireAMP\X.X.X\ipsupporttool.exe

Passo 7: Encontre o arquivo `policy.xml`, e rebatize o arquivo a `policy.xml.old`.



Passo 8: Mova o `policy.xml` transferido no diretório e clique então o **serviço de Startthe** no indicador dos serviços. O conector de FireAMP é agora debuga dentro o modo e dados de diagnóstico adicionais dos logs.



A fim desabilitar debugar o modo, execute a etapa 5 com etapa 8, desabotoar as mudanças a `policy.xml.old`, e reinicie o conector de FireAMP.