

# Collecte de données diagnostiques d'une exécution de connecteur de FireAMP sur Windows

## Contenu

[Introduction](#)

[Générez le fichier diagnostique](#)

[Mode de debug](#)

[Mode de debug d'enable](#)

[Incapable d'activer le mode de debug](#)

## Introduction

Ce document décrit les étapes pour générer un fichier diagnostique d'un connecteur de FireAMP. Si vous éprouvez un problème technique avec un connecteur de FireAMP qui fonctionne sur Microsoft Windows, un ingénieur de support technique de Cisco pourrait vouloir analyser les messages de log disponibles dans un fichier diagnostique.

## Générez le fichier diagnostique

La personne à charge sur la version de Windows, navigation à l'outil de diagnostic de support du connecteur de FireAMP pourrait être différente. Dans des la plupart des systèmes d'exploitation Windows, vous allez au menu de démarrage afin de trouver l'outil de diagnostic de support du connecteur de FireAMP. Exemple :

**Début > tous les programmes > connecteur de FireAMP > outil de diagnostic de support.**

**Note:** Si vous exécutez Windows avec le contrôle de compte utilisateur, cliquez sur **oui** afin de permettre à l'outil pour s'exécuter.

L'outil de diagnostic de support crée un fichier compressé dans le format 7z et l'enregistre sur l'appareil de bureau. Voici un exemple du nom du fichier d'un fichier diagnostique sur un appareil de bureau :

v5.0 et plus tôt : Sourcefire\_Support\_Tool\_YYYY\_MM\_DD\_HH\_MM\_SS.7z

v5.1 et plus nouveau : CiscoAMP\_Support\_Tool\_YYYY\_MM\_DD\_HH\_MM\_SS.7z

Alternativement, vous pouvez exécuter ce fichier exécutable en tant qu'administrateur :

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

## Mode de debug

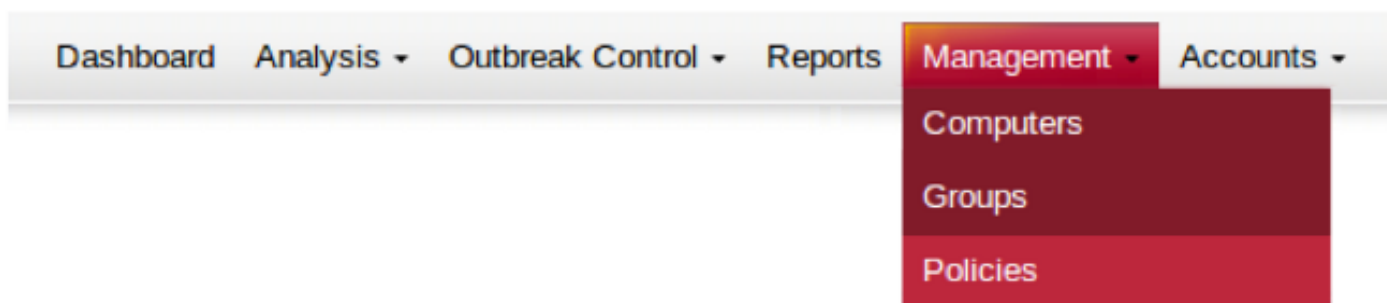
L'activation de mettre au point le mode sur un connecteur de FireAMP fournit la verbosité supplémentaire à se connecter, qui laisse plus de vue dans des problèmes avec le connecteur. Cette section décrit comment activer mettre au point le mode dans un connecteur de FireAMP.

**Avertissement** : Le mode de debug devrait être activé seulement si un ingénieur de support technique de Cisco demande ces données. L'activation mettre au point le mode pendant un plus long temps peut remplir l'espace disque très rapidement et pourrait empêcher le fichier diagnostique de support de recueillir le **log de connecteur** et le **log de barre d'état** dus à la taille de fichier excessive.

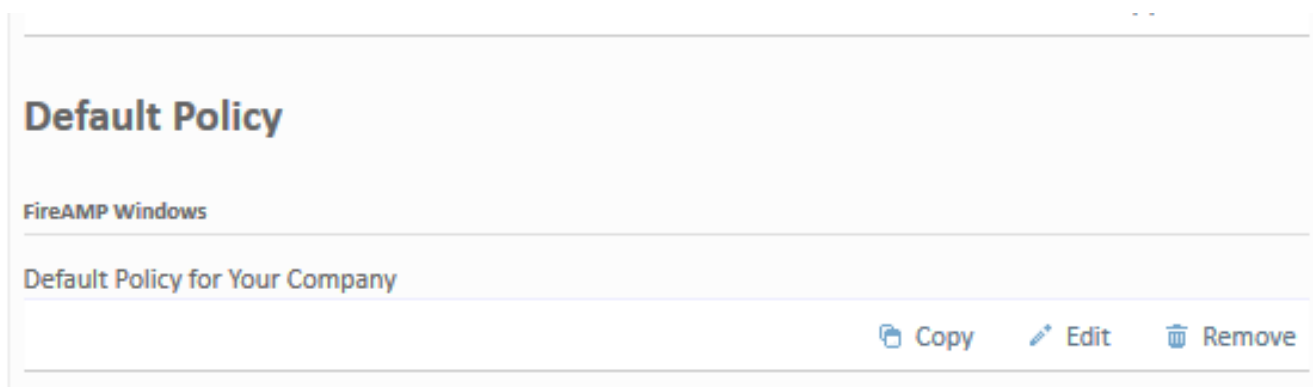
## Mode de debug d'enable

**Étape 1** : Connectez-vous dans la console de FireAMP.

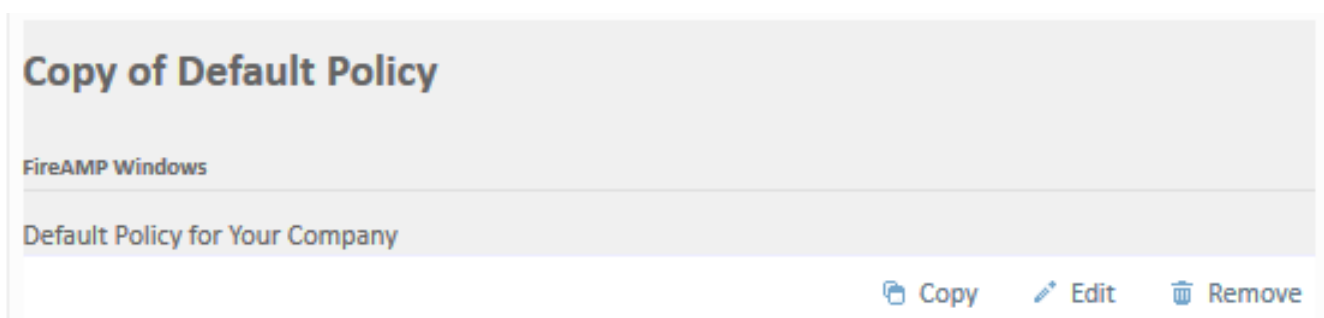
**Étape 2** : Choisissez la **Gestion > les stratégies**.



**Étape 3** : Localisez la stratégie qui est appliquée au périphérique ou à l'ordinateur d'extrémité et cliquez sur la copie.



**Étape 4** : Après que vous cliquez sur la copie, les mises à jour de console de FireAMP avec la stratégie copiée.



L'étape 5: Click **éditent** et puis cliquent sur les **caractéristiques administratives**.

## 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"/>	<a href="#">i</a>
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"/>	

**Étape 6 :** Pour le **niveau de log de barre d'état** et le **niveau de log de connecteur**, choisissez le **debug** des listes déroulantes.

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	.....	

[Étape 7](#) : Stratégie de mise à jour de clic afin de sauvegarder les modifications.

### Edit FireAMP Windows Policy

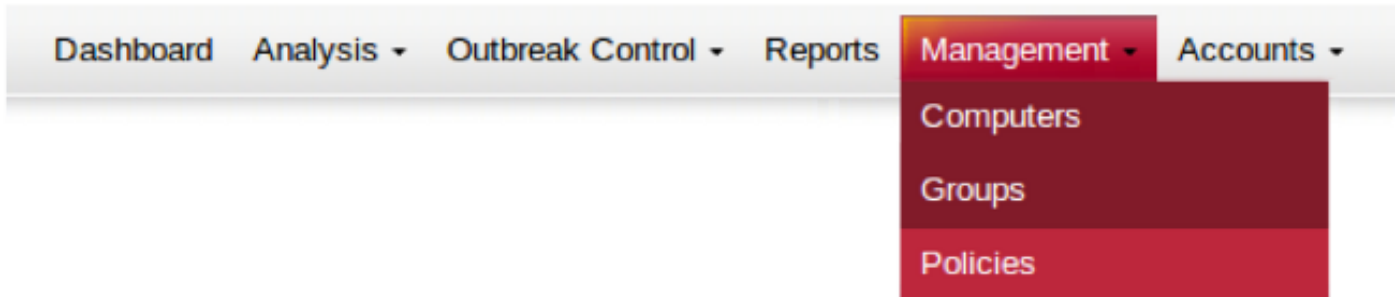
Name	Copy of Default Policy
Custom Whitelist	None
Application Block Lists	None
Simple Custom Detections	None
Advanced Custom Signatures	None
Custom Exclusion Set	Exclusions for 'Default Policy'
IP Black/White Lists	Edit
Description	Default Policy for Your Company

[Étape 8](#) : Après que vous mettiez à jour la stratégie, vous devez appliquer ceci sur le périphérique d'extrémité où vous voulez se produire mettez au point les informations.

**Incapable d'activer le mode de debug**

En raison du problème de connectivité, si vous ne pouvez pas appliquer la stratégie à un connecteur de FireAMP vous ne pourrez pas activer le mode de débogage. Dans ce cas, vous pouvez télécharger le fichier `policy.xml` et configurer le connecteur de FireAMP pour utiliser votre stratégie modifiée. Suivez ces instructions si le nuage de FireAMP ne peut pas communiquer avec le connecteur de FireAMP :

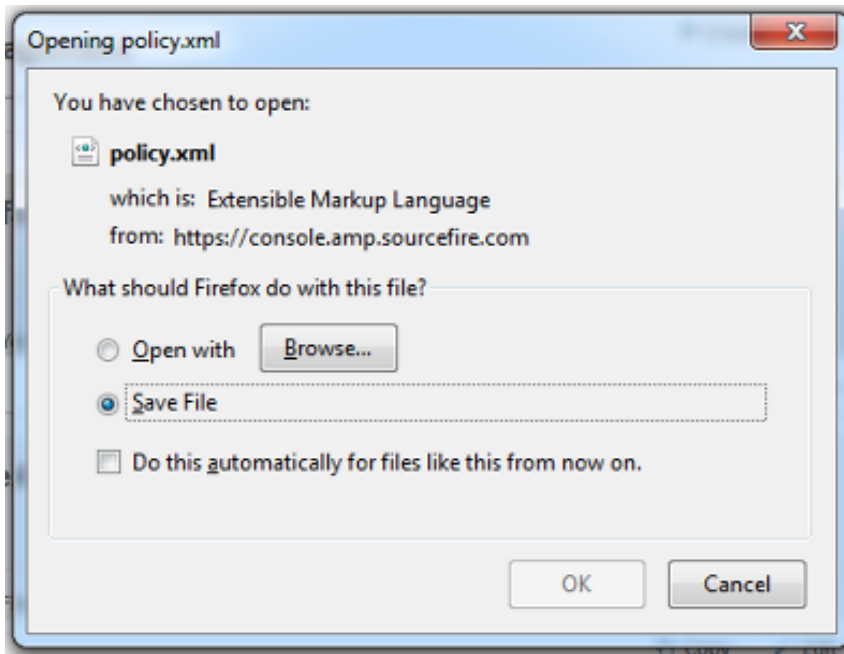
**Étape 1 :** Choisissez la **Gestion > les stratégies**.



**Étape 2 :** Localisez la stratégie qui a été copiée et cliquez sur en fonction le nom afin d'afficher le résumé de stratégie.

A screenshot of the FireAMP Policy Management interface. On the left, a list of policies is shown under the heading 'Policy Management'. The selected policy is 'Copy of Default Policy'. On the right, the detailed view of this policy is shown, including its name, last modified date, last applied status, and a 'Download Policy XML File' button. Below this, there are tabs for 'General', 'File', and 'Network', and a list of policy features like 'Administrative Features', 'Connector Identity Persistence', 'Client User Interface', 'Proxy Settings', and 'Product Updates'.

**Étape 3 :** Cliquez sur Download le **fichier XML de stratégie** et puis sauvegardez le fichier à votre ordinateur.



### 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

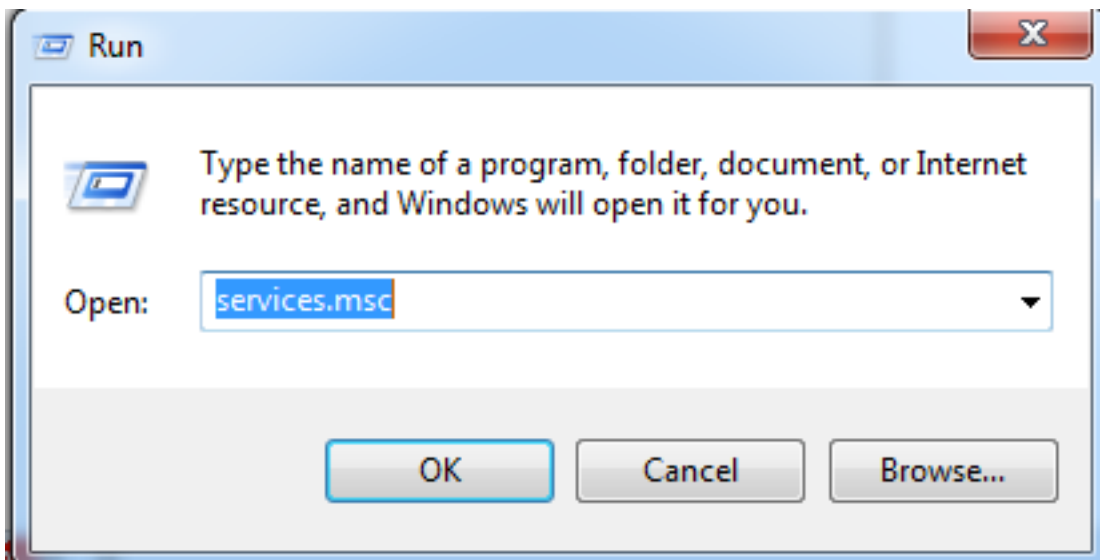
### Policy Summary

Default Policy for Your Company

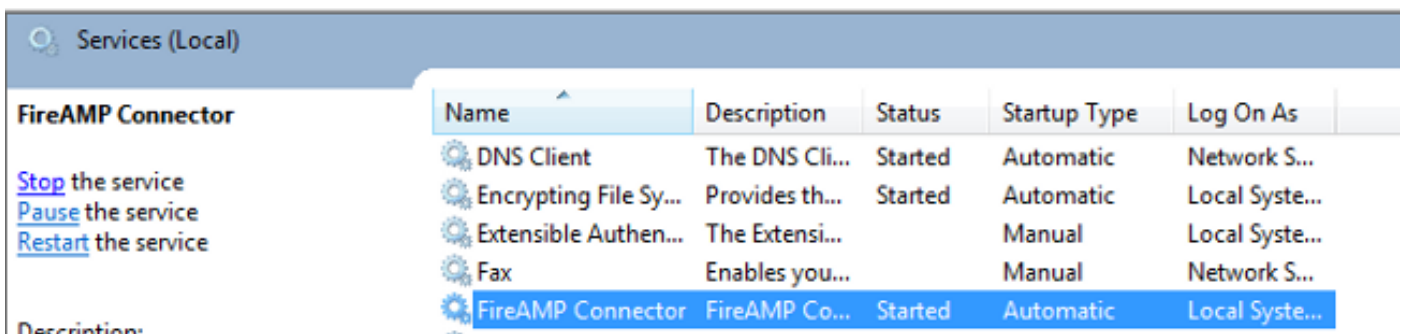
[Download Policy XML File](#)

General File Network

**Étape 4 :** Ouvrez `services.msc` avec le Start > Run.



**Étape 5 :** Localisez le service de **connecteur de FireAMP** et cliquez sur l'**arrêt**.



**Étape 6 :** Cliquez sur le **début > l'ordinateur**, puis naviguez vers un de ces répertoires selon l'architecture informatique :

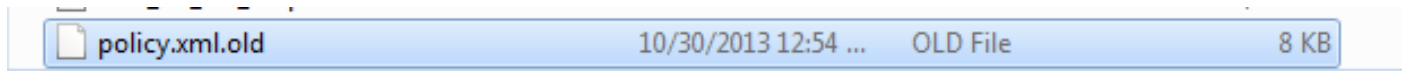
Dans la plateforme x86 :

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

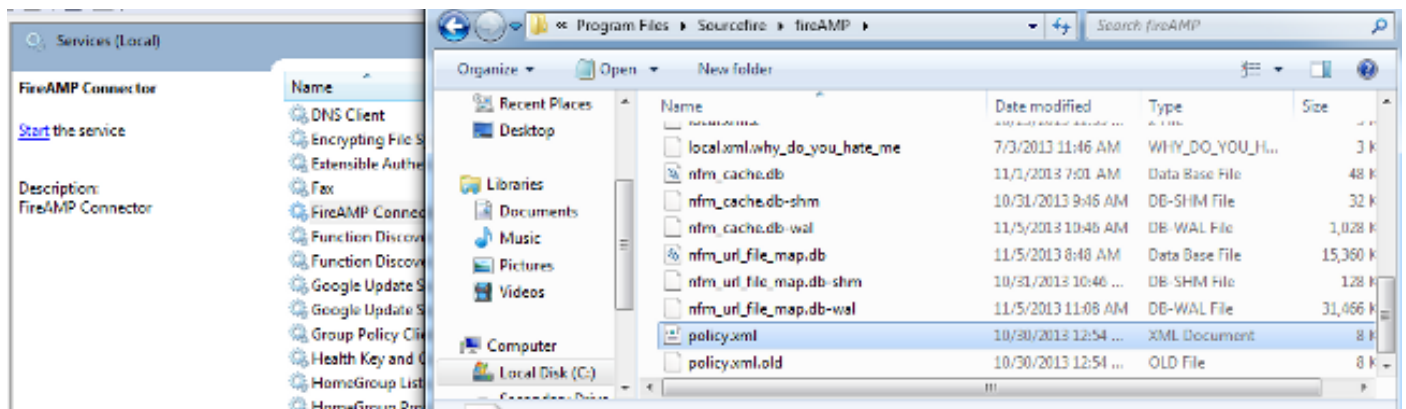
Dans la plate-forme x64 :

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

**Étape 7 :** Localisez le fichier `policy.xml`, et renommez le fichier à `policy.xml.old`.



**Étape 8 :** Entrez le `policy.xml` téléchargé dans le répertoire et puis cliquez sur le **service de Startthe** dans la fenêtre de services. Le connecteur de FireAMP est maintenant dans le mode et les données diagnostiques supplémentaires de logs.



Afin de désactiver mettez au point le mode, exécutez l'étape 5 à l'étape 8, annulez les modifications à `policy.xml.old`, et redémarrez le connecteur de FireAMP.