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.

> Remarque: 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 :

```
Sourcefire_Support_Tool_2016_01_15_10_44_11.7z
```

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

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

Mode de debug

L'activation de mettent 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 mettent 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 mettent 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.

Après que vous exécutiez l'outil de diagnostic de support dedans mettez au point le mode, les informations supplémentaires est enregistré dans des ces fichiers :

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

Ces fichiers sont enregistrés dans le répertoire de `fireAMP` situé sous le répertoire de `fichiers de programme`. Dans cet exemple, `3.x.x` est la version du connecteur de FireAMP installé sur l'hôte.

Dans des Plateformes x86 :

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

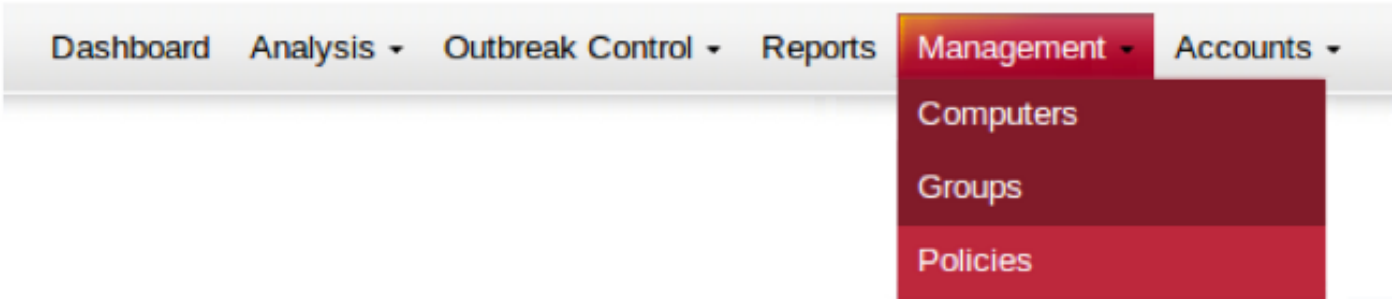
Dans des Plateformes x64 :

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

Mode de debug d'enable

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

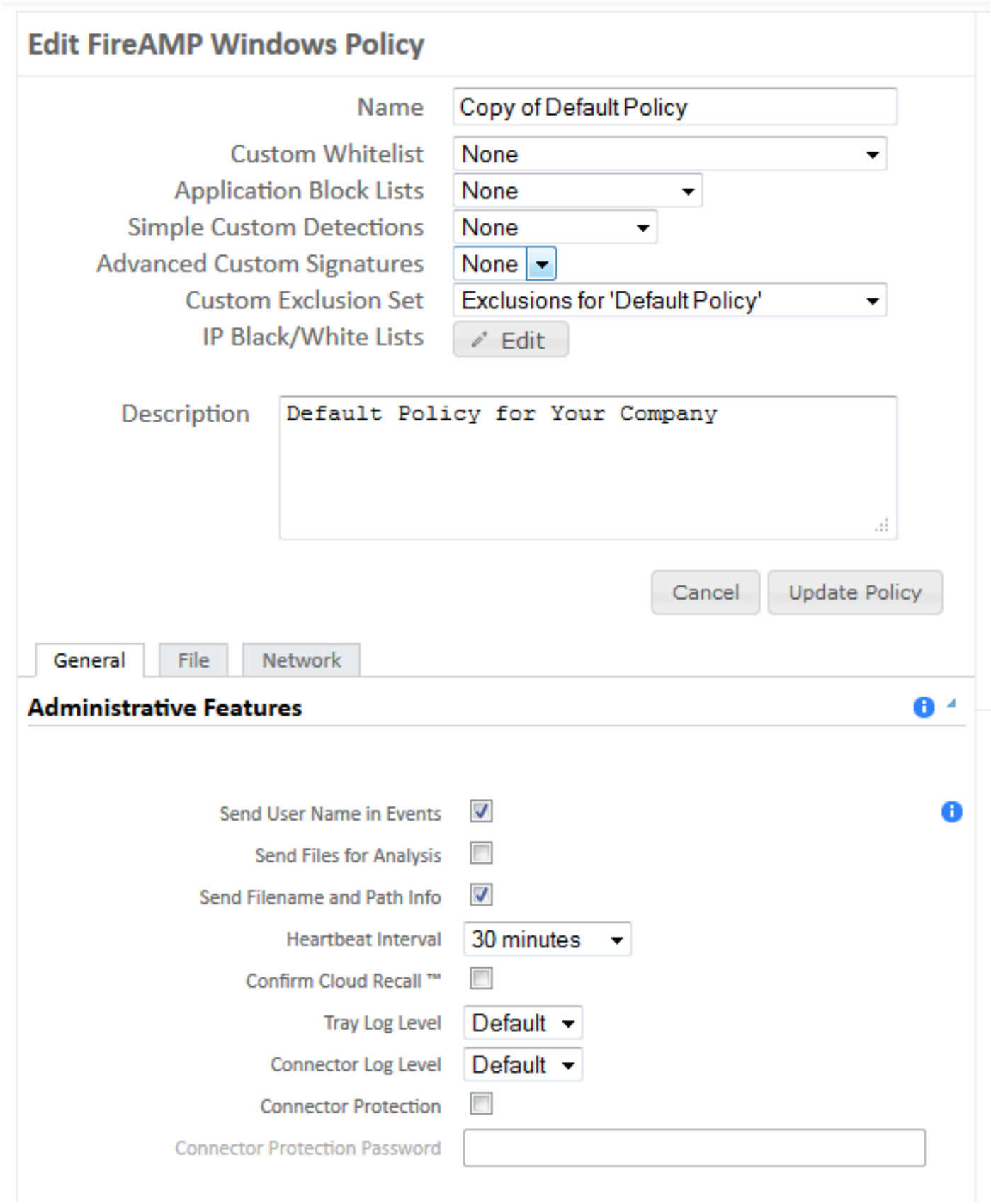
Étape 2 : Choisissez la **Gestion > les stratégies**.



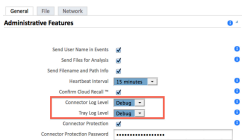
Étape 3 : Localisez la stratégie qui est appliquée au périphérique ou à l'ordinateur d'extrémité et cliquez sur la **copie.**

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

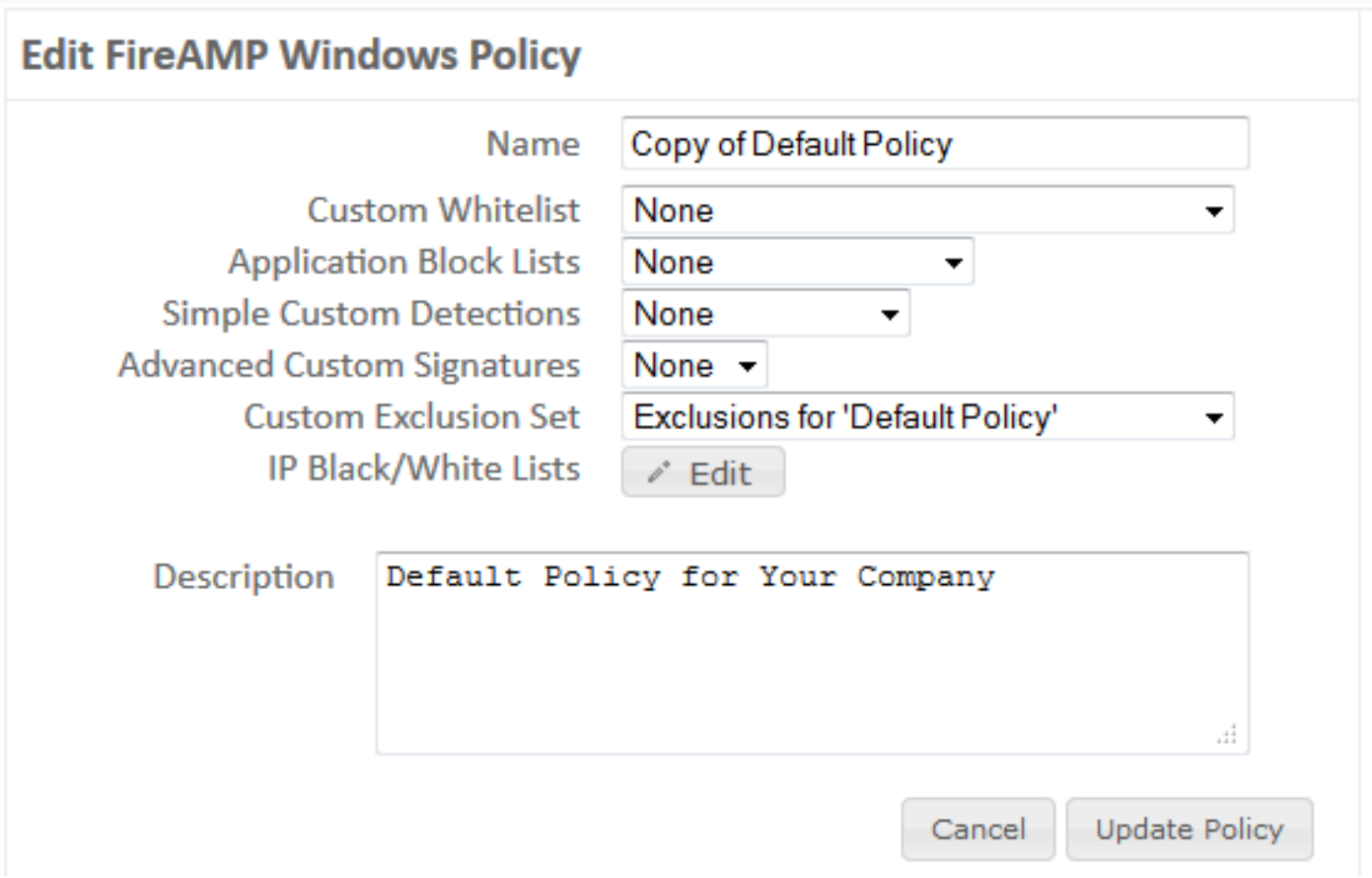
L'étape 5:Click **éditent** et puis cliquent sur les **caractéristiques administratives**.



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



Étape 7 : **Stratégie de mise à jour de** clic afin de sauvegarder les modifications.

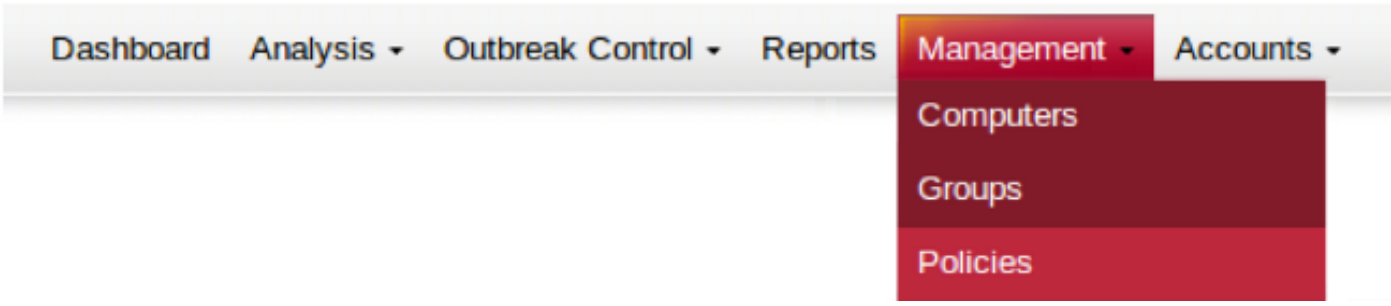


Étape 8 : Après que vous mettiez à jour la stratégie, vous devez appliquer ceci sur le périphérique d'extrémité où vous voulez se produire mettez au point les informations.

Incapable d'activer le mode de debug

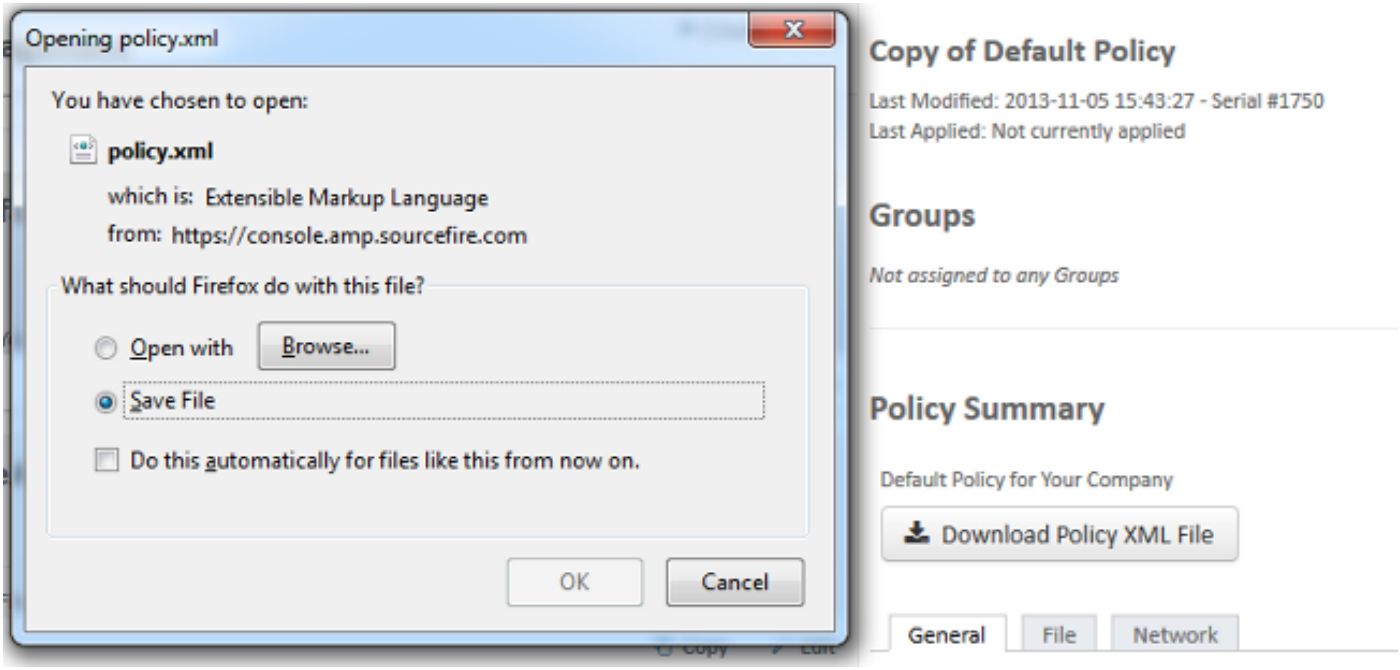
En raison du problème de connectivité, si vous ne pouvez pas appliquer la stratégie à un connecteur de FireAMP vous ne pourrez pas activer le mode de débogage. Dans ce cas, vous pouvez télécharger le `fichier policy.xml` et configurer le connecteur de FireAMP pour utiliser votre stratégie modifiée. Suivez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

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

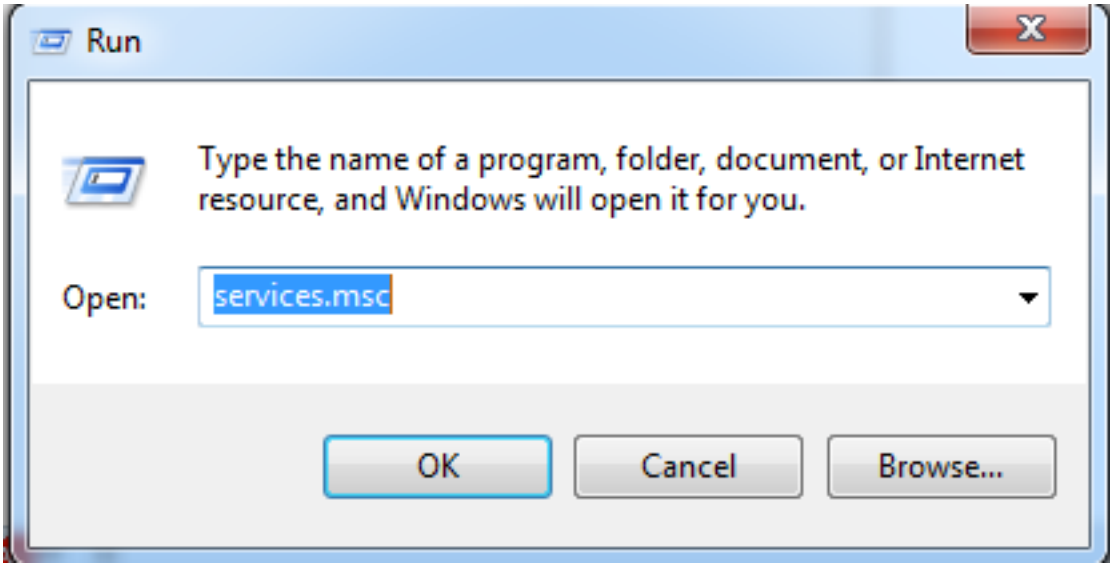


Étape 2 : Localisez la stratégie qui a été copiée et cliquez sur en fonction le nom afin d'afficher le **résumé de stratégie**.

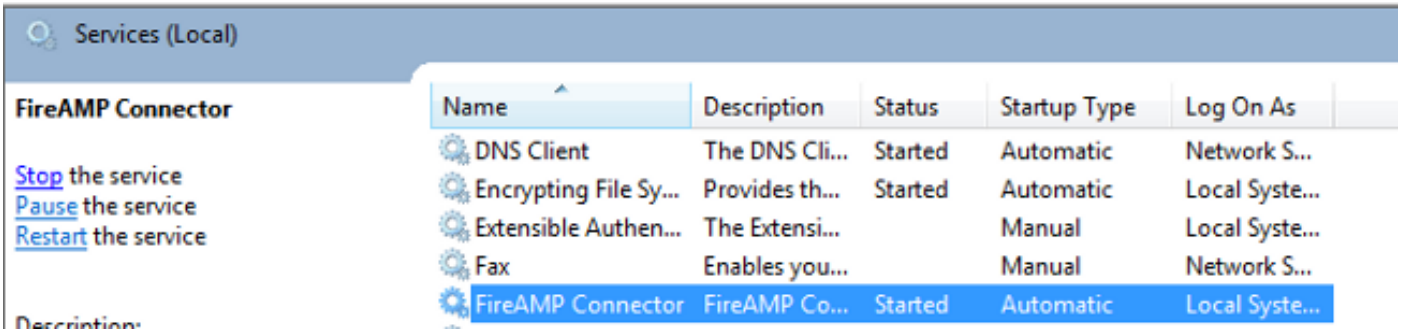
Étape 3 : Cliquez sur Download le **fichier XML de stratégie** et puis sauvegardez le fichier à votre ordinateur.



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 :

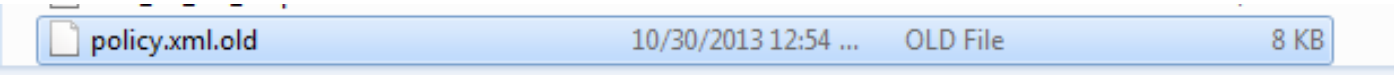
Dans la plateforme x86 :

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

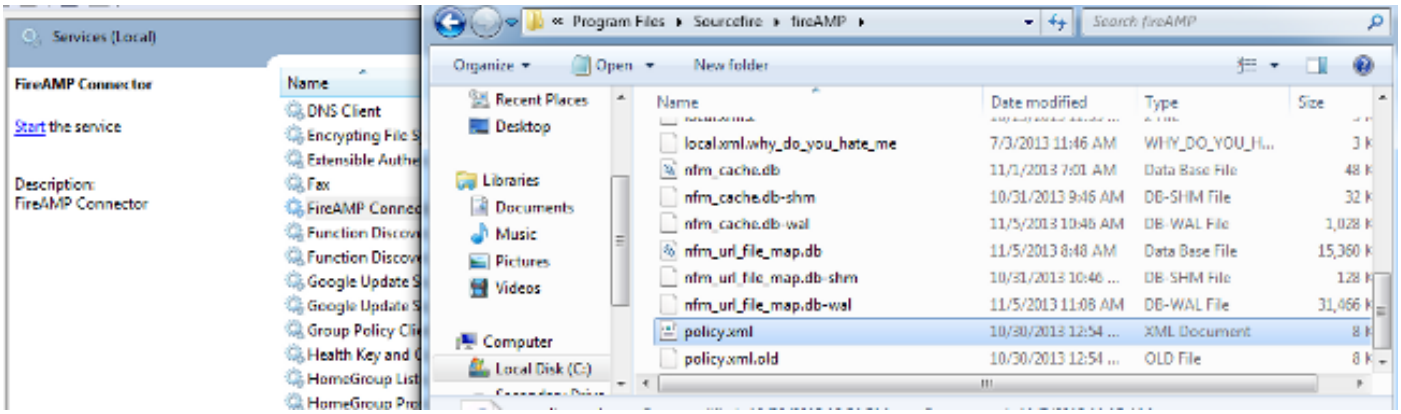
Dans la plate-forme x64 :

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

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 mettent au point maintenant dedans 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.