Colección de datos diagnósticos de un conector de FireAMP que se ejecuta en Windows

Contenido

Introducción

Este documento describe los pasos para generar un archivo de diagnóstico de un conector de FireAMP. Si usted experimenta un problema técnico con un conector de FireAMP que se ejecute en Microsoft Windows, un ingeniero de soporte técnico de Cisco pudo querer analizar los mensajes del registro disponibles en un archivo de diagnóstico.

Genere el archivo de diagnóstico

El dependiente sobre la versión de Windows, navegación a la herramienta de diagnóstico del soporte del conector de FireAMP pudo ser diferente. En la mayoría de los sistemas operativos Windows, usted va al menú Inicio para encontrar la herramienta de diagnóstico del soporte del conector de FireAMP. Por ejemplo:

Comienzo > todos los programas > conector de FireAMP > herramienta de diagnóstico del soporte.

> **Note**: Si usted ejecuta Windows con el control de cuentas de usuario, haga clic **sí** para permitir que la herramienta se ejecute.

La herramienta de diagnóstico del soporte crea un archivo comprimido en el formato 7z y lo guarda en el escritorio. Aquí está un ejemplo del nombre de fichero de un archivo de diagnóstico en un escritorio:

v5.0 y anterior: `Sourcefire_Support_Tool_YYYY_MM_DD_HH_MM_SS.7z`

v5.1 y más nuevo: `CiscoAMP_Support_Tool_YYYY_MM_DD_HH_MM_SS.7z`

Alternativamente, usted puede funcionar con este archivo ejecutable como administrador:

```
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
```

Modo del debug

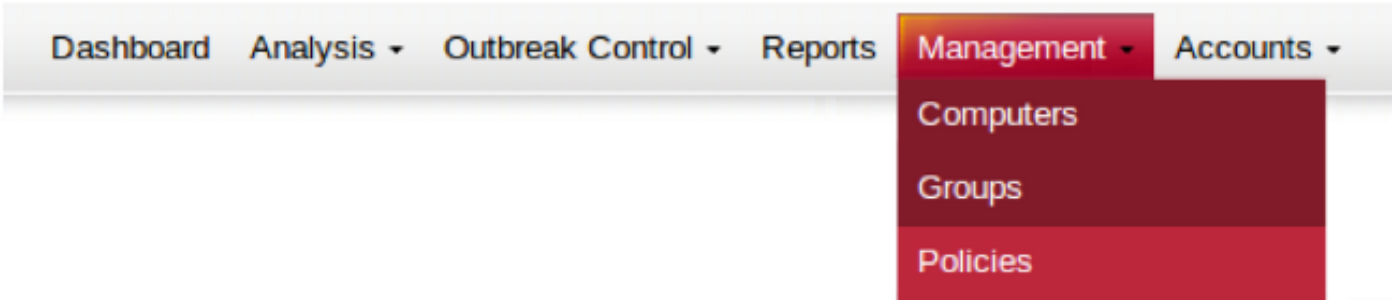
La habilitación del modo del debug en un conector de FireAMP proporciona la verbosidad adicional al registro, que permite más penetración en los problemas con el conector. Esta sección describe cómo habilitar el modo del debug en un conector de FireAMP.

> Advertencia: El modo del debug debe ser habilitado solamente si un ingeniero de soporte técnico de Cisco pide estos datos. Habilitar el modo del debug por un tiempo más largo puede llenar el espacio en disco muy rápidamente y pudo evitar que el archivo de diagnóstico del soporte recolecte el **registro del conector** y el **registro de la bandeja** debido al tamaño del archivo excesivo.

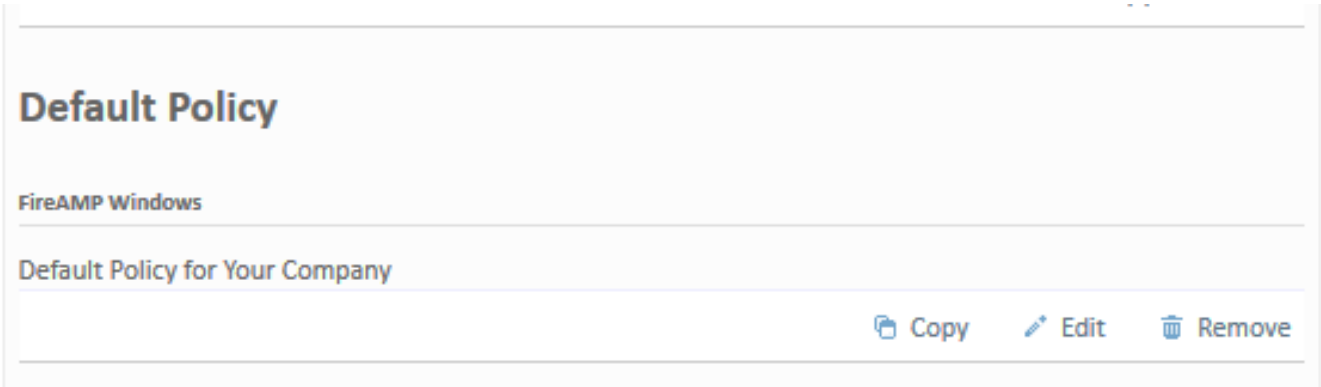
Modo del debug del permiso

Paso 1: Registro en la consola de FireAMP.

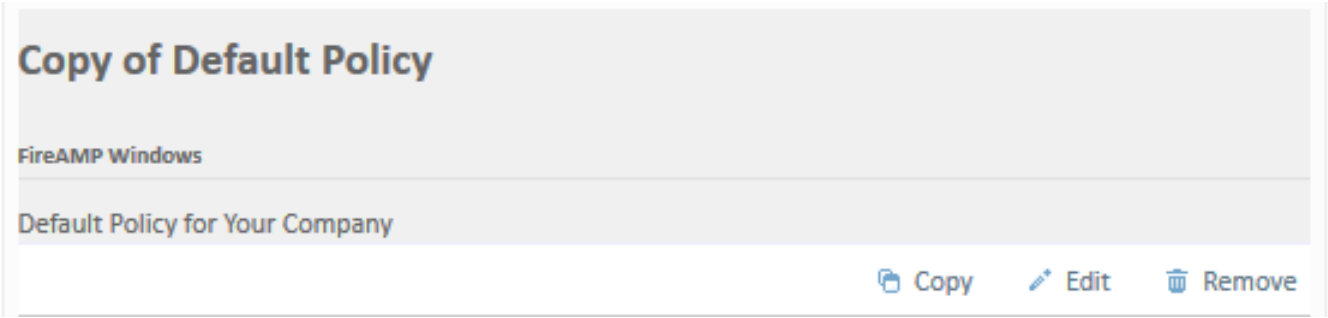
Paso 2: Elija la **Administración > las directivas**.



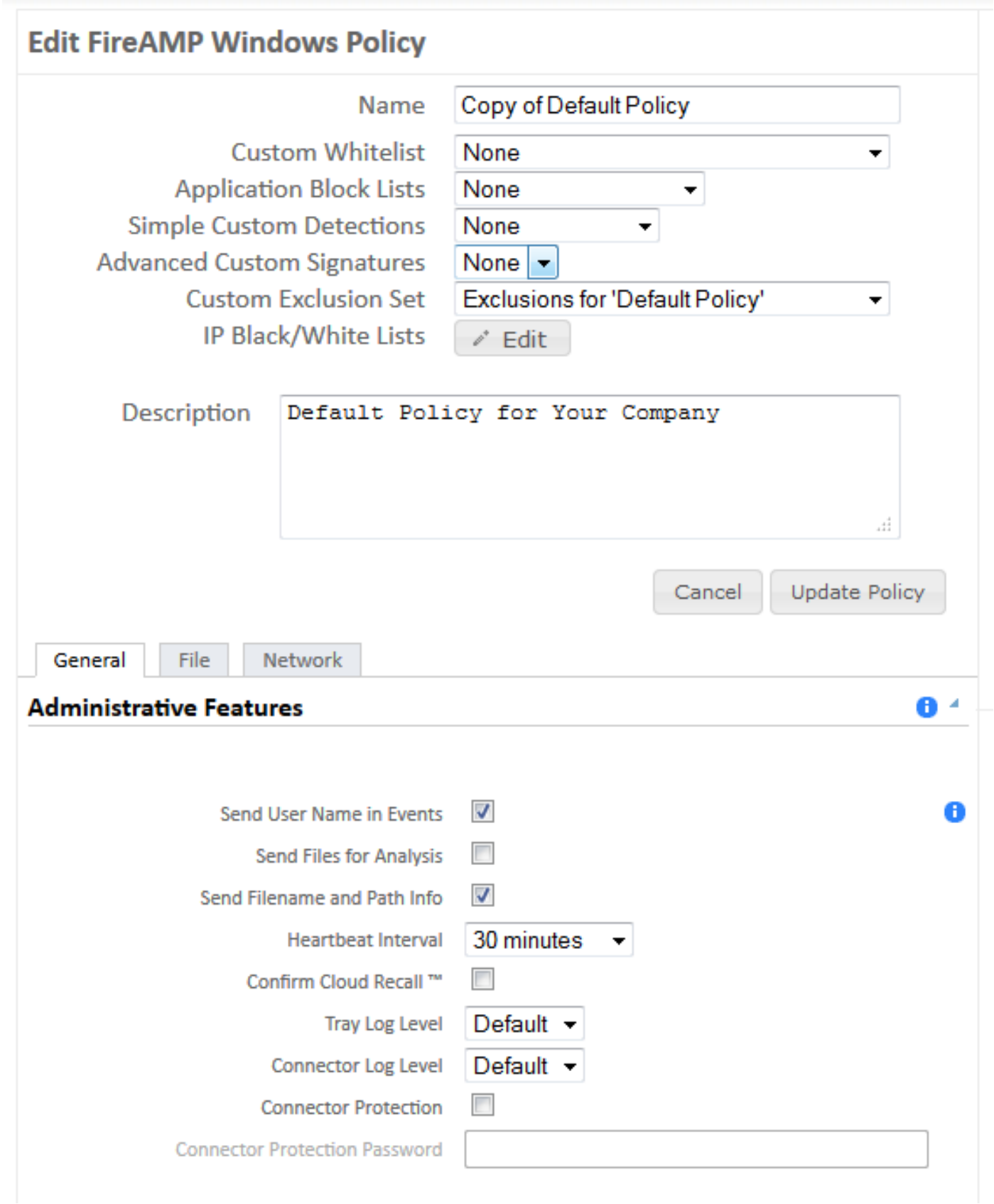
Paso 3: Localice la directiva que es al final dispositivo u ordenador aplicado y haga clic la **copia.**



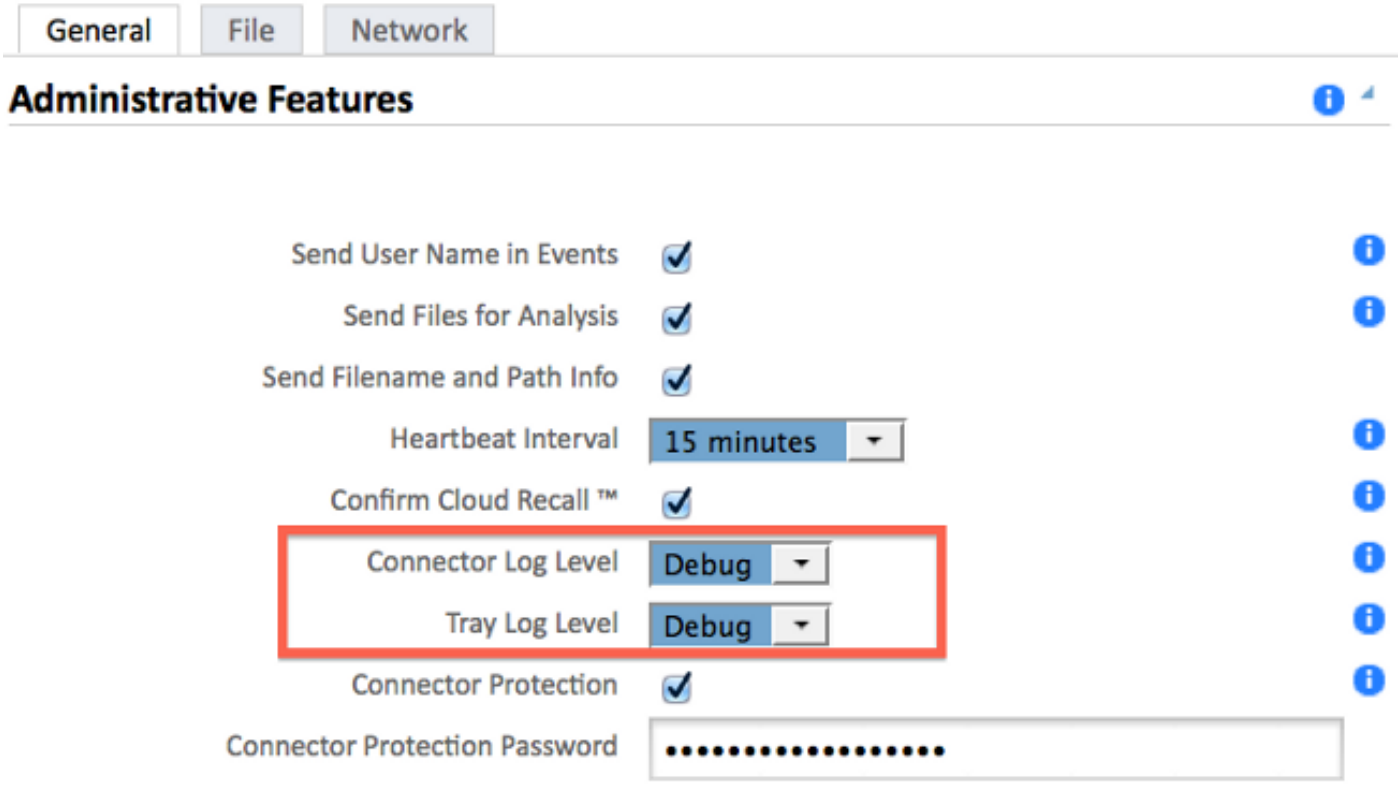
Paso 4: Después de que usted haga clic la copia, las actualizaciones de la consola de FireAMP con la directiva copiada.



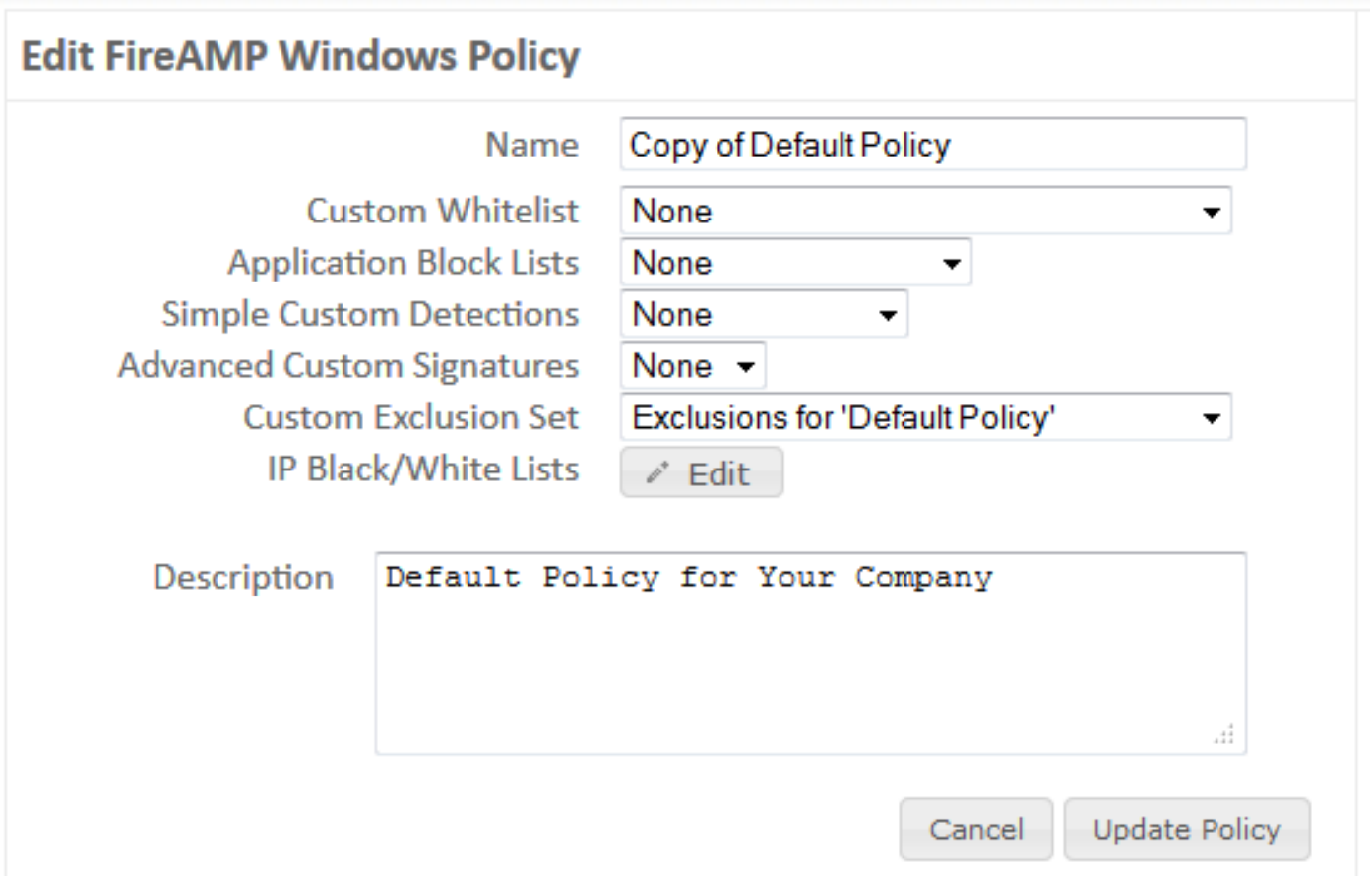
El paso 5:Click **edita** y después hace clic las **características administrativas**.



Paso 6: Para el **nivel del registro de la bandeja** y el **nivel del registro del conector**, elija el **debug de las** listas desplegables.



Paso 7: **Directiva de la actualización del** tecleo para salvar los cambios.

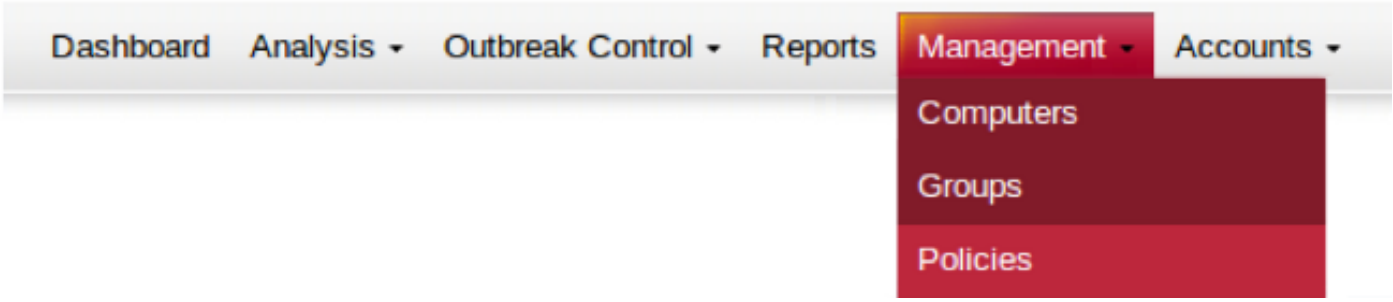


Paso 8: Después de que usted ponga al día la directiva, usted necesita aplicar esto en el dispositivo extremo donde usted quiere generar la información del debug.

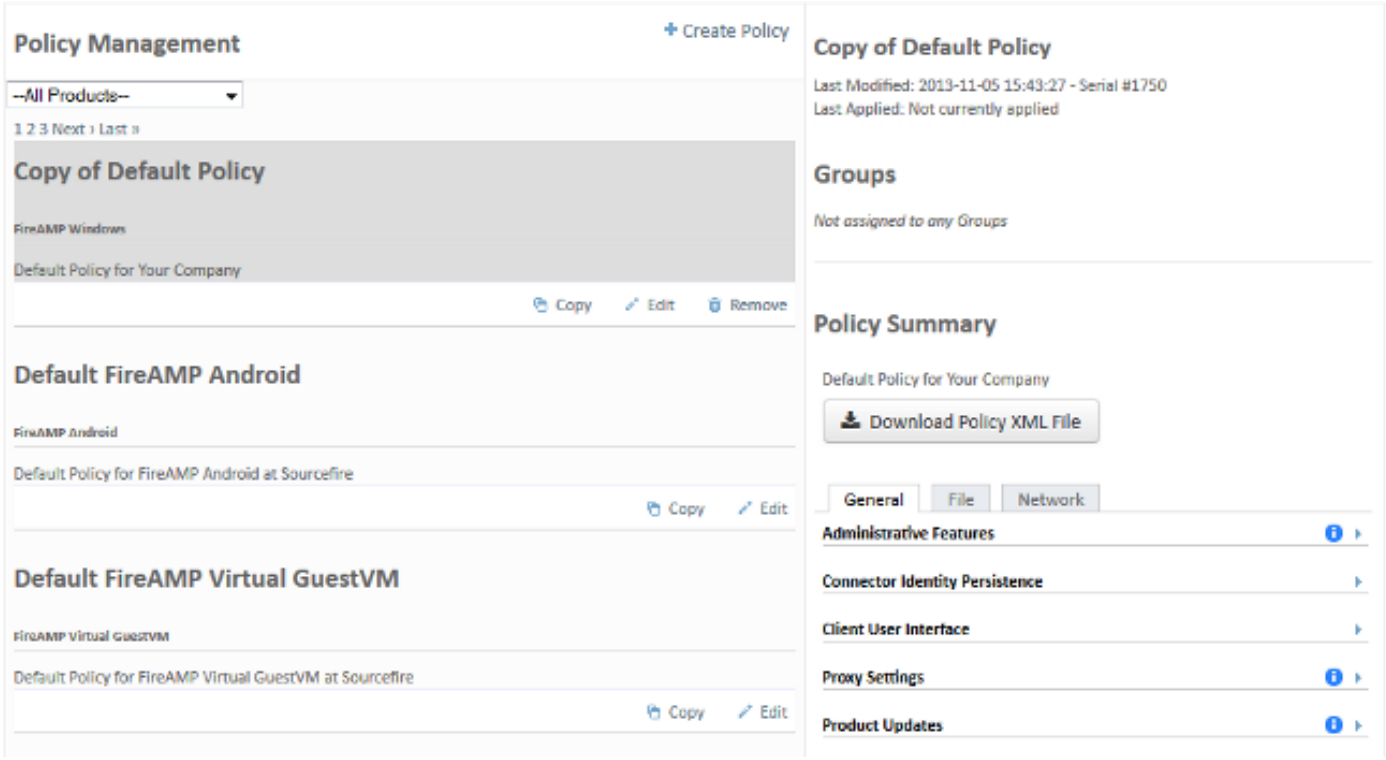
Incapaz de habilitar el modo del debug

Debido al problema de conectividad, si usted no puede aplicar la directiva a un conector de FireAMP usted no podrá habilitar el modo del debug. En ese caso, usted puede descargar el `archivo policy.xml` y configurar el conector de FireAMP para utilizar su directiva modificada. Siga estas instrucciones si la nube de FireAMP no puede comunicar con el conector de FireAMP:

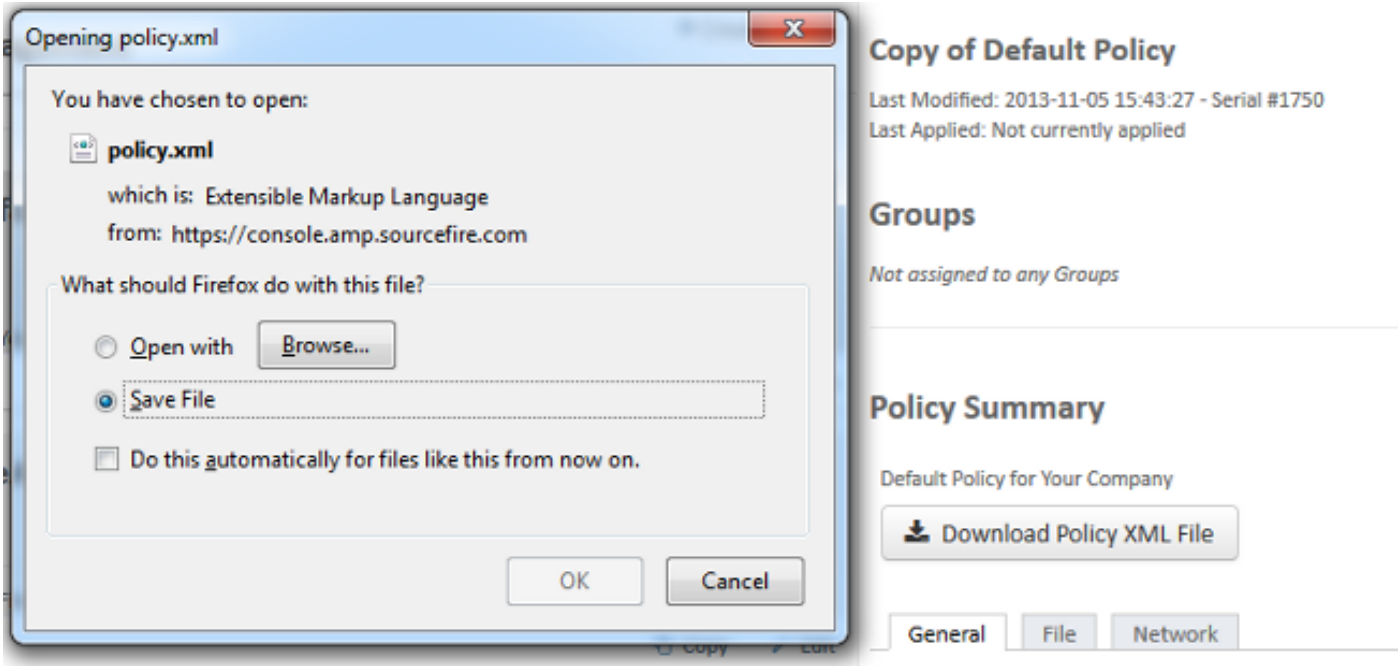
Paso 1: Elija la **Administración > las directivas**.



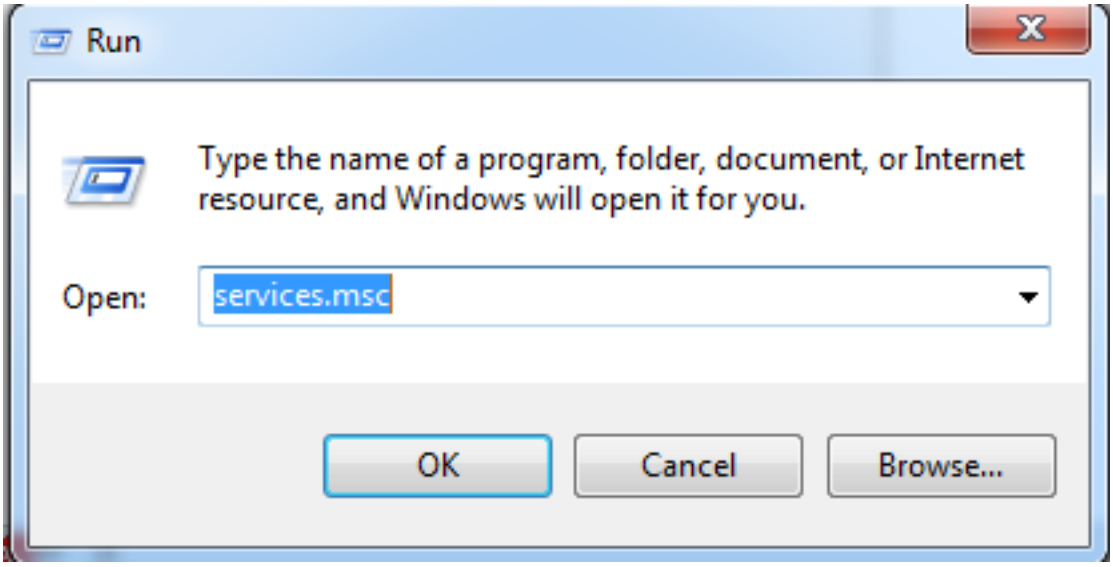
Paso 2: Localice la directiva que fue copiada y haga clic en el nombre para visualizar el **resumen de la directiva**.



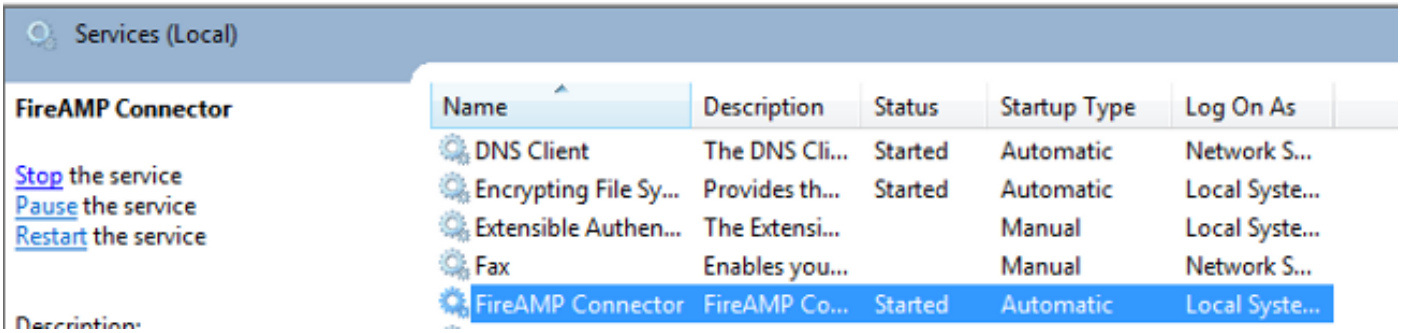
Paso 3: Haga clic el **archivo XML de la directiva de la descarga** y después salve el archivo a su ordenador.



Paso 4: Abra **`services.msc` con el** Start (Inicio) > Run (Ejecutar).



Paso 5: Localice el servicio del **conector de FireAMP** y haga clic la **parada**.



Paso 6: Haga clic el **comienzo > la Computadora**, después navegue a uno de estos directorios dependiendo de la arquitectura de ordenador:

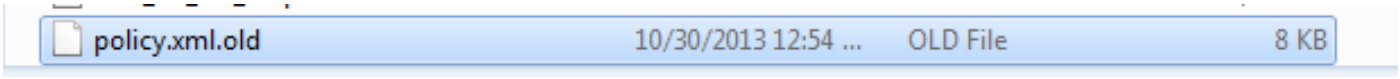
En la plataforma del x86:

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

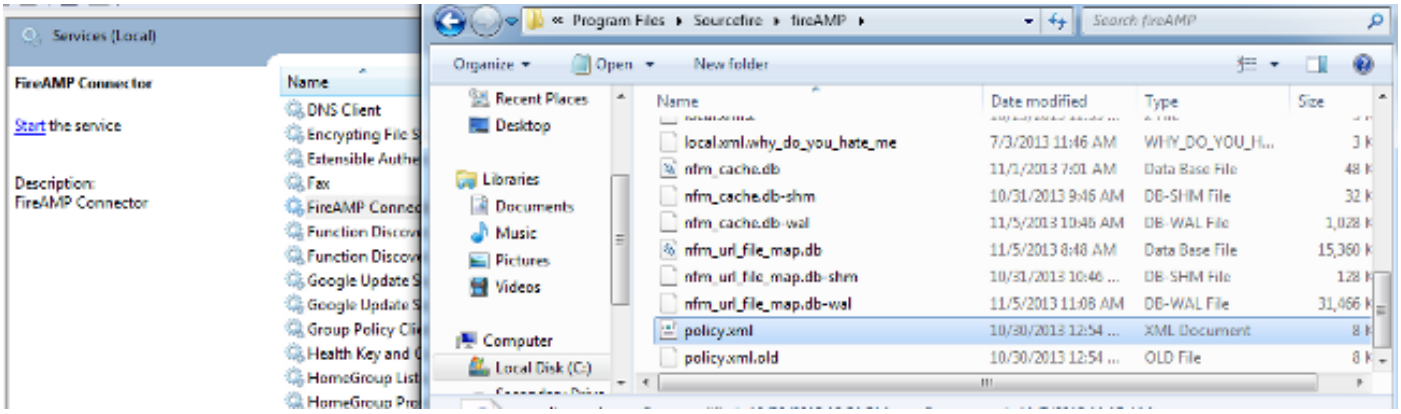
En la plataforma x64:

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

Paso 7: Localice el archivo `policy.xml, y` retitule el archivo a policy.xml.old.



Paso 8: Trasládese el `policy.xml` descargado al directorio y después haga clic el **servicio de** Startthe **en la** ventana de los servicios. El conector de FireAMP ahora es adentro modo del debug y datos diagnósticos adicionales de los registros.



Para inhabilitar el modo del debug, realice el paso 5 al paso 8, deshaga los cambios a `policy.xml.old, y recomience el` conector de FireAMP.