

La imagen o reproduce una Computadora con el conector de FireAMP instalado

Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Preinstalación - Versiones 4.1.4 y más alto](#)

[Poste-instalación - Versiones 4.1.4 y más alto](#)

[Preinstalación - Las versiones bajan que 4.1](#)

[Poste-instalación - Las versiones bajan que 4.1](#)

Introducción

Este documento describe los procesos para prevenir las varias computadoras para intentar el uso lo mismo global - el Identificador único (GUID), que previene los objetos duplicados del ordenador para aparecer en el panel de la nube de FireAMP. Este proceso permite que FireAMP trabaje correctamente en una máquina reproducida.

Como administrador de sistema, usted puede querer incluir el conector de FireAMP en sus imágenes principales del PC de Windows. FireAMP, sin embargo, requiere que los sistemas puedan ser identificados únicamente. Los pasos generales para reproducir una máquina para Linux están en la parte inferior de este artículo.

Nota: El primer conjunto de las instrucciones se aplica a la versión 4.1.4 o posterior de FireAMP. Usted encuentra más lejos los pasos originales para las máquinas que funcionan con las versiones anteriores.

Prerrequisitos

Requisitos

No hay requisitos específicos para este documento.

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando,

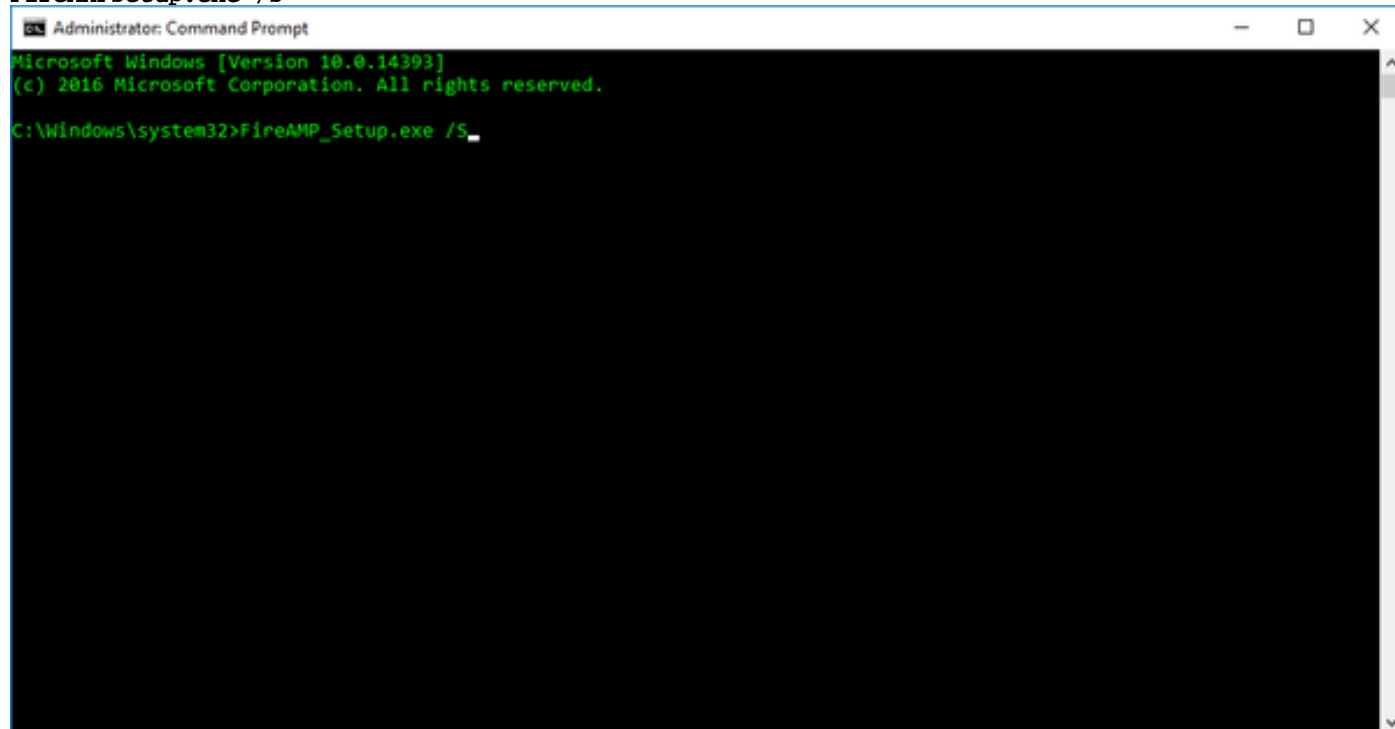
asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Preinstalación - Versiones 4.1.4 y más alto

Realice estos pasos para preparar un ordenador para la proyección de imagen:

Paso 1. Instale FireAMP en su imagen principal.

FireAMPSetup.exe /s

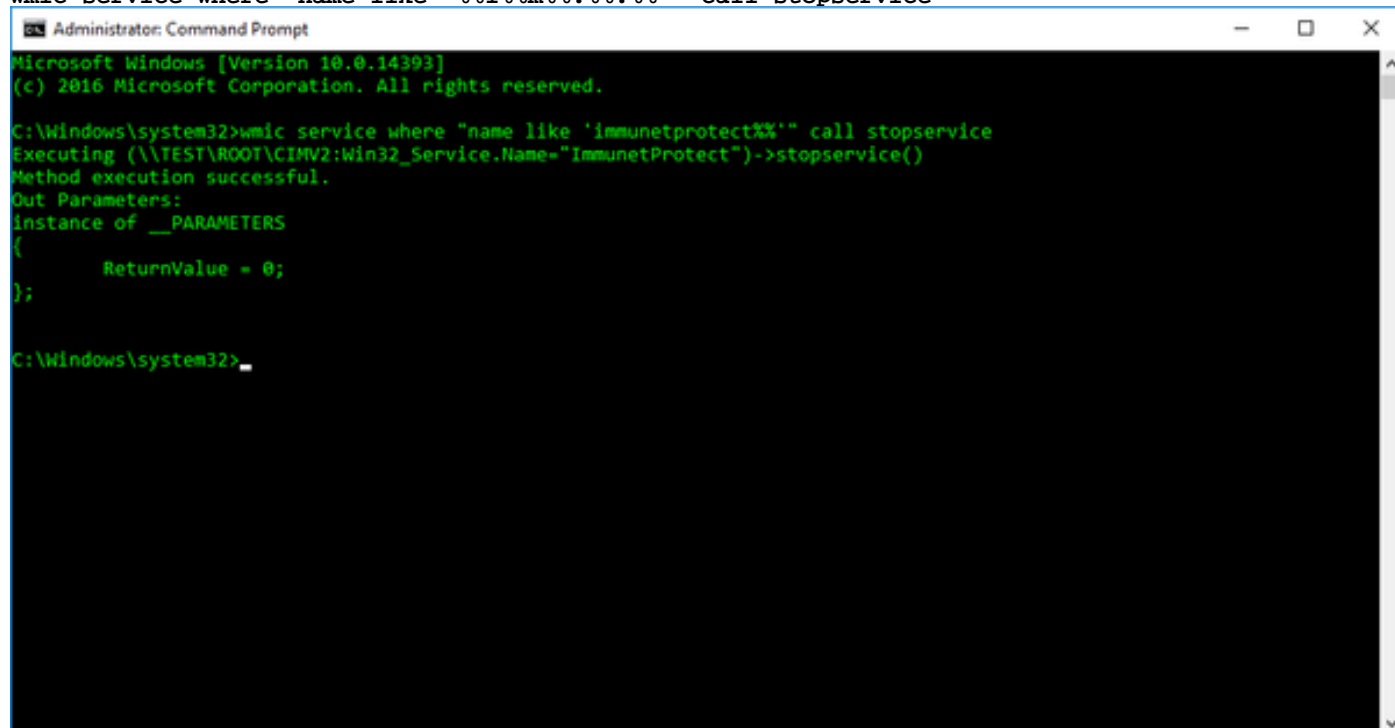


```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Windows\system32>FireAMP_Setup.exe /s_
```

Paso 2. Pare el servicio de FireAMP.

wmic service where "name like '%i%m%.%.%' " call stopservice



```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Windows\system32>wmic service where "name like 'immnetprotect%'" call stopservice
Executing (\\TEST\ROOT\CIMV2:Win32_Service.Name="ImmnetProtect")->stopservice()
Method execution successful.
Out Parameters:
instance of __PARAMETERS
{
    ReturnValue = 0;
};

C:\Windows\system32>_
```

Utilice el siguiente comando si usted hace la protección del conector habilitar. La contraseña será visible en el comando prompt.

4.2 and Lower: Not Available

4.3 to 5.0: "%PROGRAMFILES%\Sourcefire\fireAMP\X.X.X\sfc.exe" -k protectionpassword

5.1 and Above: "%PROGRAMFILES%\Cisco\AMP\X.X.X\sfc.exe" -k protectionpassword

Nota: Si el servicio de FireAMP se comienza otra vez, la imagen principal regenera **local.xml**. Usted necesita relanzar estos pasos para neutralizar la imagen principal otra vez. Esté seguro de incluir estos pasos en su proceso de la preparación de la imagen principal.

Paso 3. Cancelación local.xml.

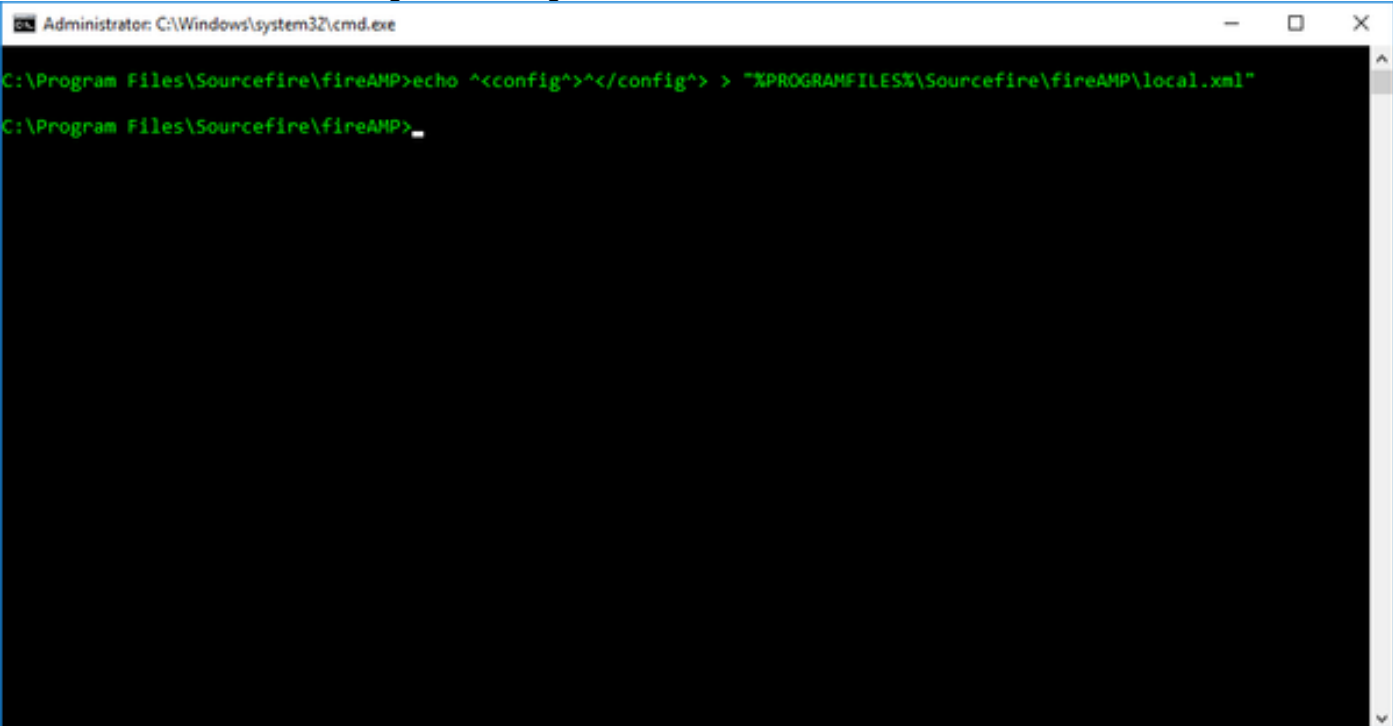
5.0 and Lower: del "%PROGRAMFILES%\Sourcefire\fireAMP\local.xml"

5.1 and Above: del "%PROGRAMFILES%\Cisco\AMP\local.xml"

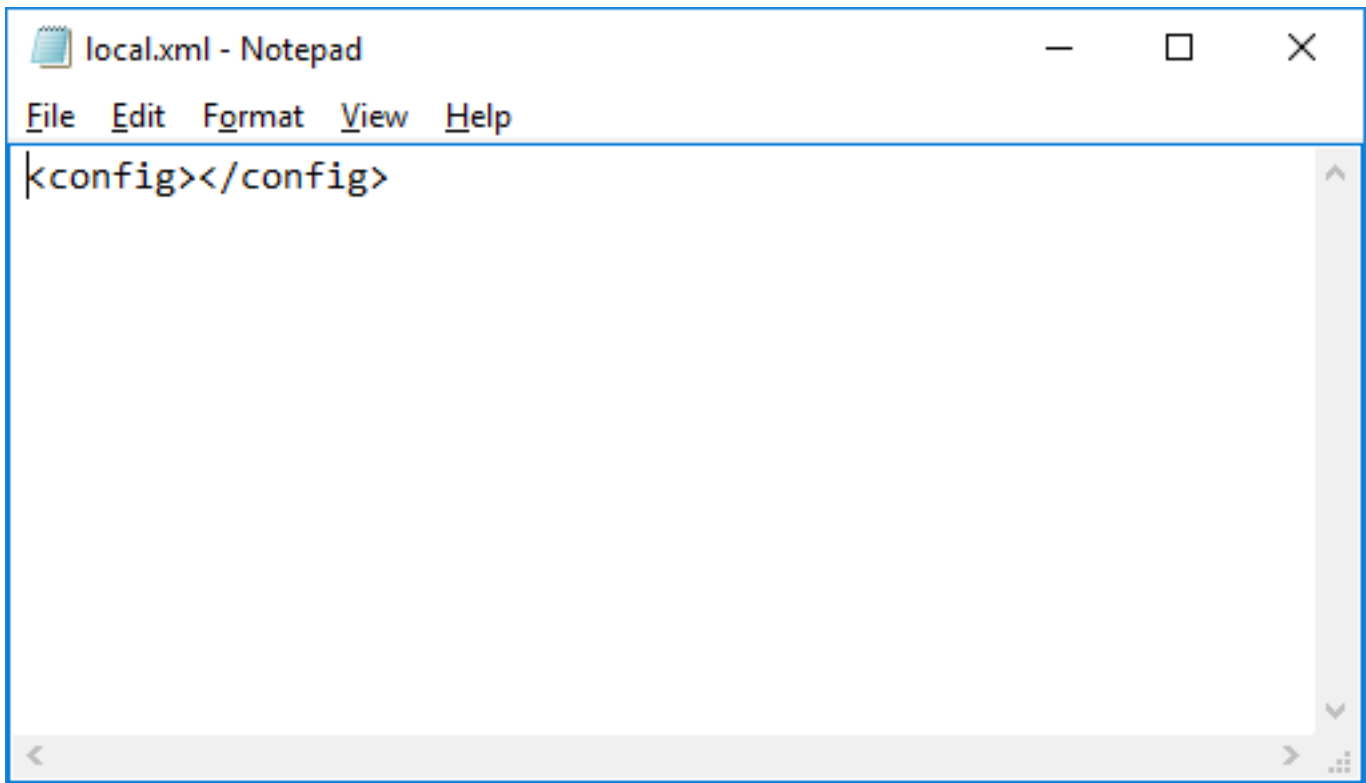
Paso 4. Cree un archivo en blanco local.xml.

5.0 and Lower: echo ^<config^>^</config^> > "%PROGRAMFILES%\Sourcefire\fireAMP\local.xml"

5.1 and Above: echo ^<config^>^</config^> > "%PROGRAMFILES%\Cisco\AMP\local.xml"



The screenshot shows a Windows command prompt window titled "Administrator: C:\Windows\system32\cmd.exe". The prompt is at "C:\Program Files\Sourcefire\fireAMP>". The user has entered the command: `echo ^<config^>^</config^> > "%PROGRAMFILES%\Sourcefire\fireAMP\local.xml"`. The prompt is now at "C:\Program Files\Sourcefire\fireAMP>_".



Poste-instalación - Versiones 4.1.4 y más alto

FireAMP 4.1.4 y más alto genera automáticamente un nuevo registration y un Identificador único universal (UUID) cuando el servicio del conector detecta un **archivo** en blanco **local.xml**. No más de pasos necesitan ser realizados en la máquina sí mismo.

Nota: Se espera que las máquinas que se registran con un **archivo** en blanco **local.xml** se coloca en el grupo predeterminado de sus organizaciones. Usted debe decidir si usted quiere mover estas máquinas manualmente o cambiar su grupo predeterminado para ser el grupo deseado para esas máquinas.

En este momento el cliente de FireAMP debe ser en servicio. Usted puede utilizar la interfaz de usuario para verificar la Conectividad y eso que el servicio se está ejecutando. Si su interfaz de usuario no se fija para comenzar, puede ser comenzada manualmente con éstos comando. Está seguro de poner al día el número de la versión para su actualmente versión instalada.

5.0 and Lower: "%PROGRAMFILES%\Sourcefire\fireAMP\X.X.X\iptray.exe" -f
5.1 and Above: "%PROGRAMFILES%\Cisco\AMP\X.X.X\iptray.exe" -f



Preinstalación - Las versiones bajan que 4.1

Realice estos pasos para preparar un ordenador para la proyección de imagen:

Paso 1. Instale FireAMP en su imagen principal.

FireAMPSetup.exe /s

The image shows a Windows Command Prompt window titled "Administrator: Command Prompt". The window content is as follows:

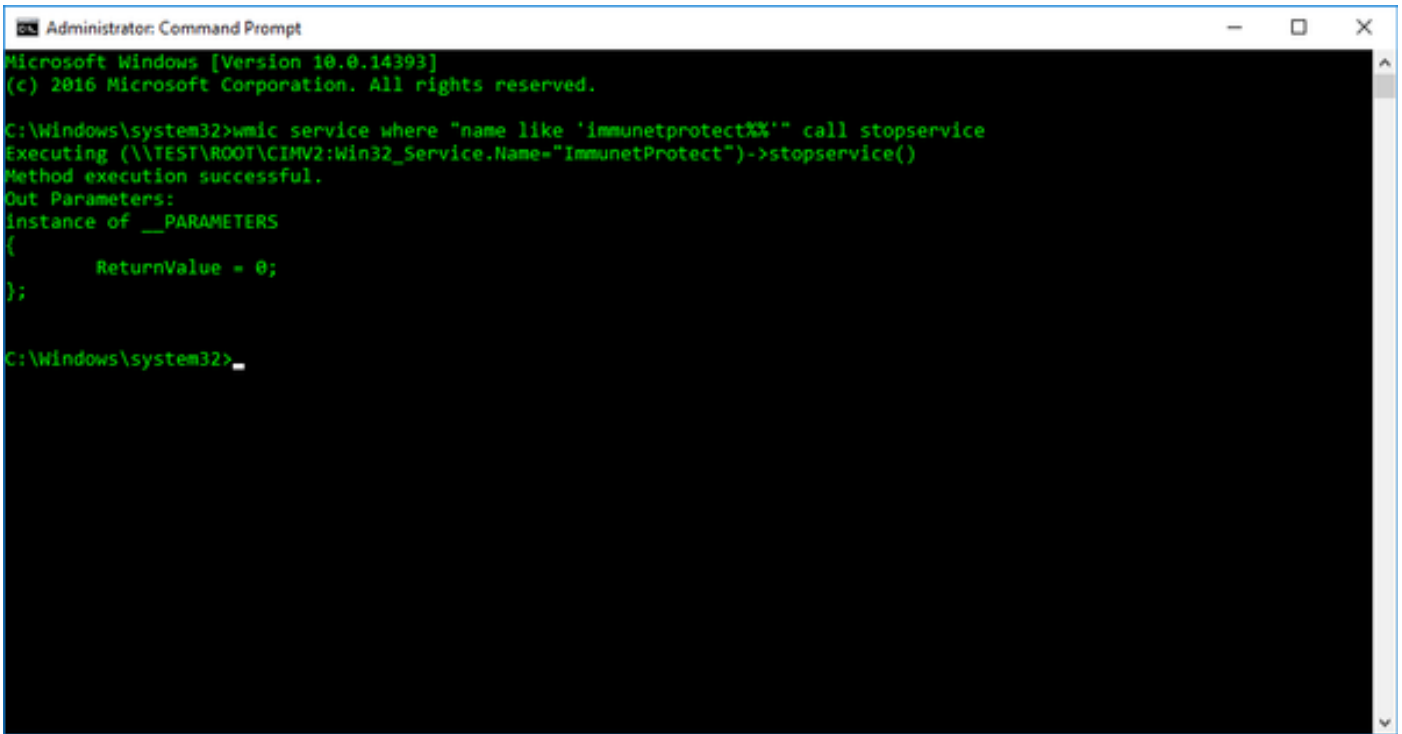
```
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Windows\system32>FireAMP_Setup.exe /s_
```

Paso 2. Pare el servicio de FireAMP.

Nota: Si usted utiliza una contraseña de la protección del conector, ésta necesita ser hecha de la interfaz de usuario.

wmic service where "name like '%i%m%.%.%'" call stopservice



```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Windows\system32>wmic service where "name like 'immunetprotect%\'" call stopservice
Executing (\\TEST\ROOT\CIMV2:Win32_Service.Name="ImmunetProtect")->stopservice()
Method execution successful.
Out Parameters:
Instance of __PARAMETERS
{
    ReturnValue = 0;
};

C:\Windows\system32>_
```

Paso 3. Determine la ubicación del producto del fireAMP. El valor por defecto es

```
%PROGRAMFILES%\Sourcefire\fireAMP
```

Paso 4. Desinstale el servicio del conector de FireAMP del panel de control ejecutando `sfc.exe` - u de la carpeta de la versión. Esté seguro de poner al día el comando con su actualmente número de la versión instalada.

```
"%PROGRAMFILES%\Sourcefire\fireAMP\4.X.X\sfc.exe" -u
```

Paso 5. Si usted quiere reutilizar el objeto existente del ordenador, usted debe respaldo el archivo existente `local.xml`. El `local.xml` es encontrado en este directorio:

```
%PROGRAMFILES%\Sourcefire\fireAMP\
```

Nota: Esto es ideal para la nueva imagen individual pero puede no ser práctico para uno-a-muchas prácticas de la proyección de imagen como salva la información única, tal como GUID de un solo ordenador.

Paso 6. Después de que usted sostenga `local.xml` o si usted no necesita reutilizar el objeto del ordenador en su panel, la cancelación `local.xml`, tal y como se muestra en de la imagen:

```
del local.xml
```

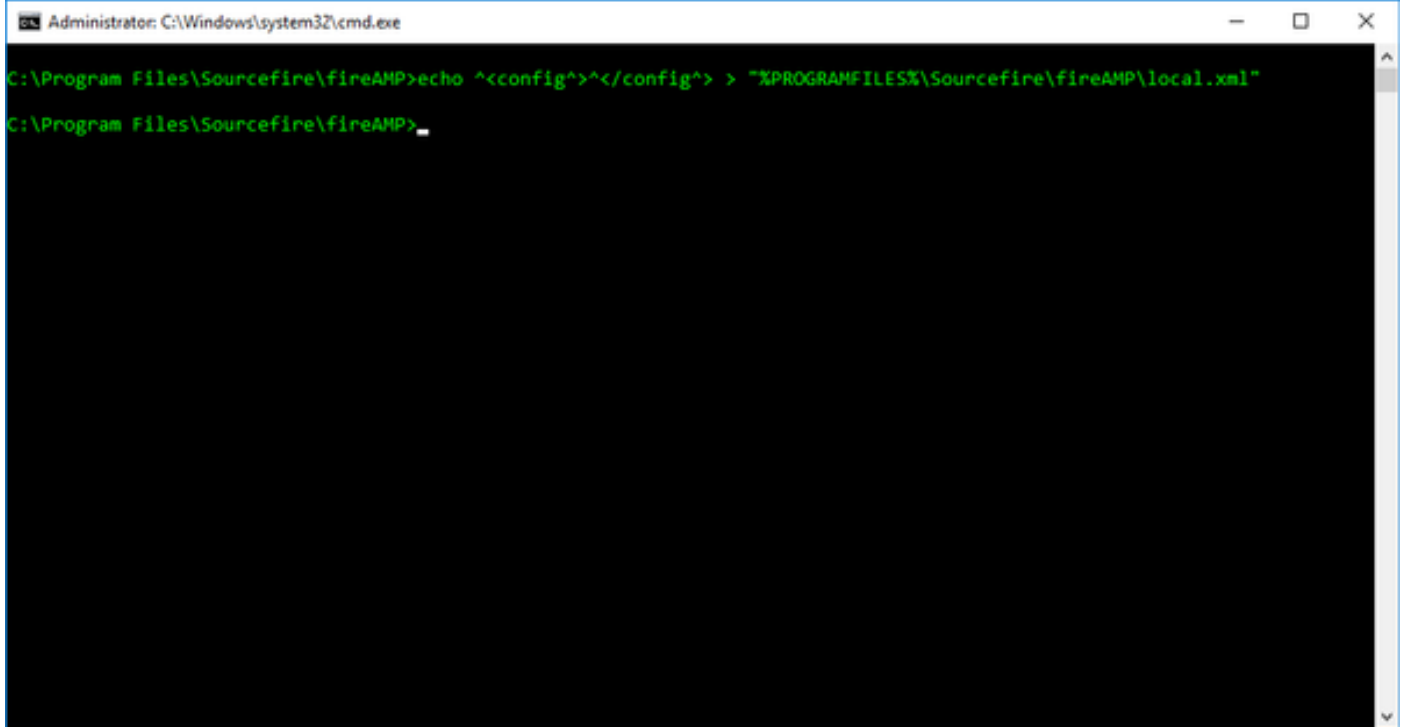
Poste-instalación - Las versiones bajan que 4.1

Realice estos pasos después de desplegar su imagen:

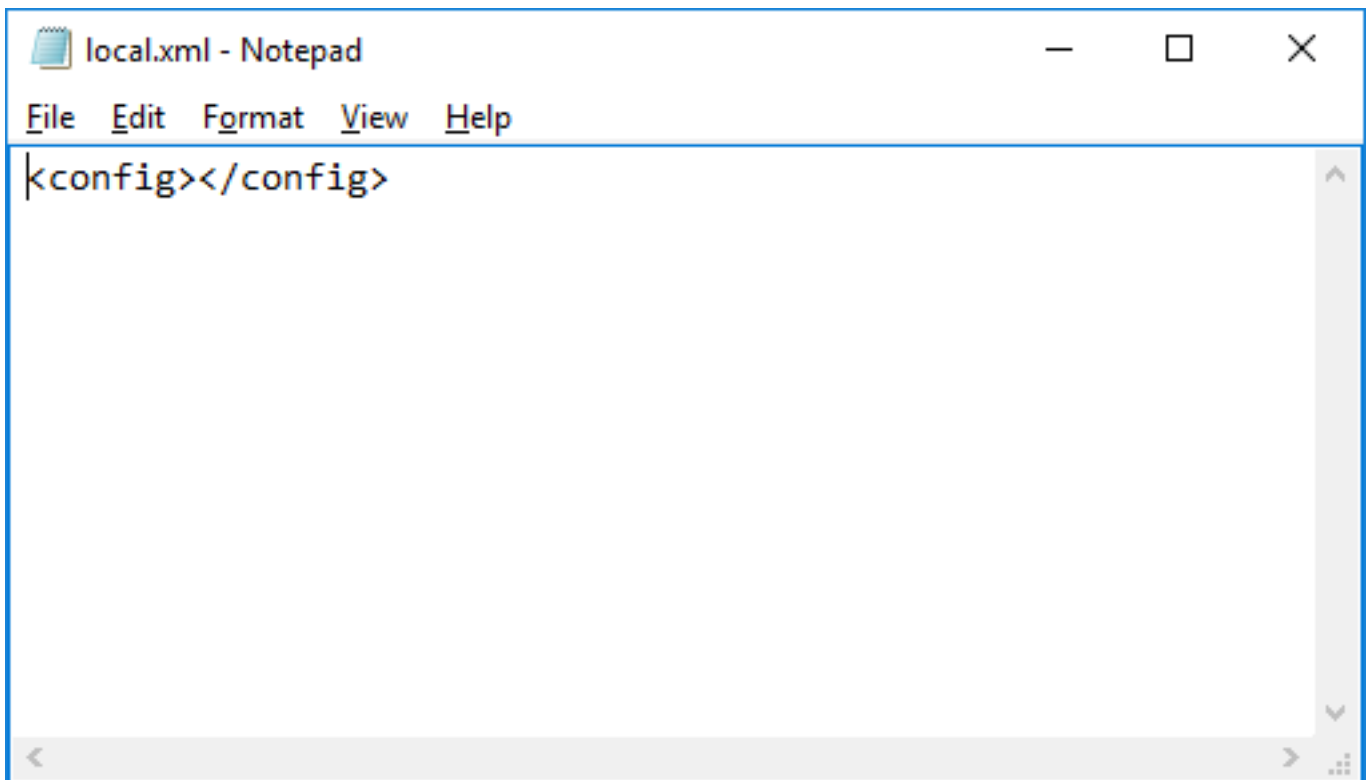
Nota: Si usted comienza el servicio de FireAMP con el archivo genérico `local.xml`, crea un nuevo objeto del ordenador. Si usted tiene el `local.xml` file original, usted puede restablecerlo por el ordenador para hacer el objeto reutilizar.

Paso 1. Restablezca el archivo `local.xml` a este directorio ahora si usted lo apoyó para arriba antes de reimaging. Si usted no restablece un `local.xml`file, usted debe todavía crear genérico para que el conector se registre correctamente.

```
echo ^<config^>^</config^> > "%PROGRAMFILES%\Sourcefire\fireAMP\local.xml"
```



The screenshot shows a Windows command prompt window titled "Administrator: C:\Windows\system32\cmd.exe". The prompt is at the directory `C:\Program Files\Sourcefire\fireAMP`. The command `echo ^<config^>^</config^> > "%PROGRAMFILES%\Sourcefire\fireAMP\local.xml"` has been entered and executed, resulting in a blank line at the prompt.



The screenshot shows a Notepad window titled "local.xml - Notepad". The menu bar includes "File", "Edit", "Format", "View", and "Help". The text content of the file is `<config></config>`.

Paso 2. Registre el conector con el servicio ejecutando el `sfc - r` de la carpeta de la versión. Este paso completa el archivo `local.xml` para un ordenador. Está seguro de poner al día los comandos abajo con su actualmente número de la versión instalada.

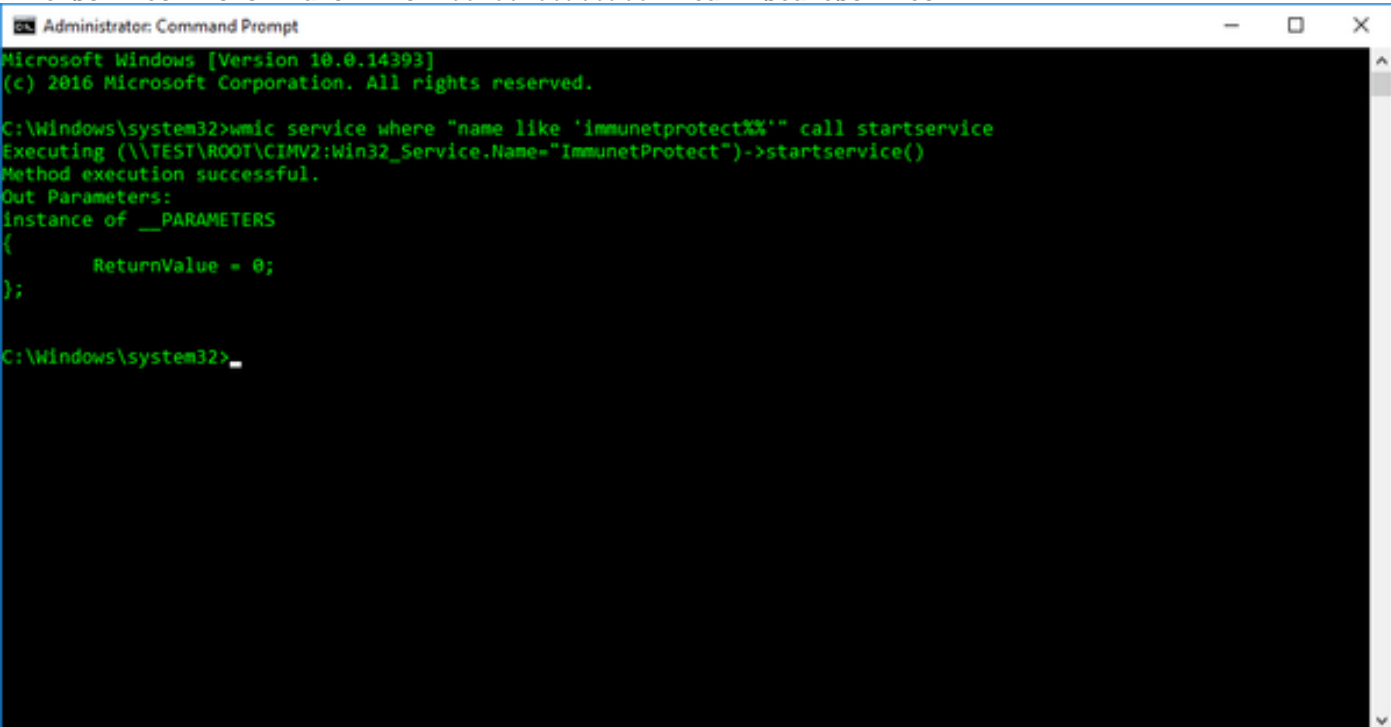
```
"%PROGRAMFILES%\Sourcefire\fireAMP\4.X.X\sfc.exe" -r
```

Instale el conector al panel de control de los servicios ejecutando `sfc.exe - i` de la carpeta de la versión.

"%PROGRAMFILES%\Sourcefire\fireAMP\4.X.X\sfc.exe" -i

Encienda el conector funcionando con el comando:

```
wmic service where "name like '%i%m%.%.%.%' " call startservice
```



```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Windows\system32>wmic service where "name like 'immunetprotect%'" call startservice
Executing (\\TEST\ROOT\CIMV2:Win32_Service.Name="ImmunetProtect")->startservice()
Method execution successful.
Out Parameters:
Instance of __PARAMETERS
{
    ReturnValue = 0;
};

C:\Windows\system32> _
```

Nota: Se espera que las máquinas que se registran manualmente de esta manera estén colocadas en el grupo predeterminado de sus organizaciones. Usted debe decidir si usted quiere mover estas máquinas manualmente o cambiar su grupo predeterminado para ser el grupo deseado para esas máquinas.

En este momento el cliente de FireAMP debe ser en servicio. Usted puede utilizar la interfaz de usuario para verificar la Conectividad y eso que el servicio se está ejecutando. Si su interfaz de usuario no se fija para comenzar, puede ser comenzada manualmente con el comando abajo. Esté seguro de poner al día el número de la versión para su actualmente versión instalada.

"%PROGRAMFILES%\Sourcefire\fireAMP\4.X.X\iptray.exe" -f



Linux

Los pasos generales para reproducir una máquina para Linux y tienen una nueva identidad son similares a Windows. Aquí están los pasos y los comandos:

Instale el amperio en su imagen principal

```
$ (sudo) yum install filename.rpm
```

Pare el servicio amperio

```
$ (sudo) initctl stop cisco-amp
```

Borre local.xml

```
$ (sudo) rm /opt/cisco/amp/etc/local.xml
```

Cuando una diversa máquina arranca con la imagen reproducida, el servicio amperio comenzará automáticamente para arriba y generará una nueva identidad. Debe ser único a través de todos los conectores de comunicación en un grupo en el [whether public, or private] de la nube.