# Instalación y configuración del módulo AMP a través de AnyConnect 4.x y AMP Enabler

## Contenido



## Introducción

Este documento sigue los pasos para instalar el conector de protección frente a malware avanzado (AMP) con AnyConnect.

AnyConnect AMP Enabler se utiliza como medio para implementar AMP para terminales. Por sí misma, no tiene ninguna capacidad para condenar la disposición de los archivos. Lleva el software AMP para terminales a un terminal de ASA. Una vez instalado AMP, utiliza la capacidad de la nube para comprobar la disposición de los archivos. Un servicio de AMP adicional puede enviar archivos a un análisis dinámico denominado ThreatGrid para obtener una puntuación del comportamiento de los archivos desconocidos. Estos archivos pueden declararse maliciosos si se cumplen ciertos artefactos. Esto es muy útil para los ataques de día cero.

## Prerequisites

### Requirements

- AnyConnect Secure Mobility Client versión 4.x
- FireAMP/AMP para terminales
- Adaptive Security Device Manager (ASDM) versión 7.3.2 o posterior

### Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Adaptive Security Appliance (ASA) 5525 con la versión de software 9.5.1
- AnyConnect Secure Mobility Client 4.2.00096 en Microsoft Windows 7 Professional de 64 bits
- ASDM versión 7.5.1(112)

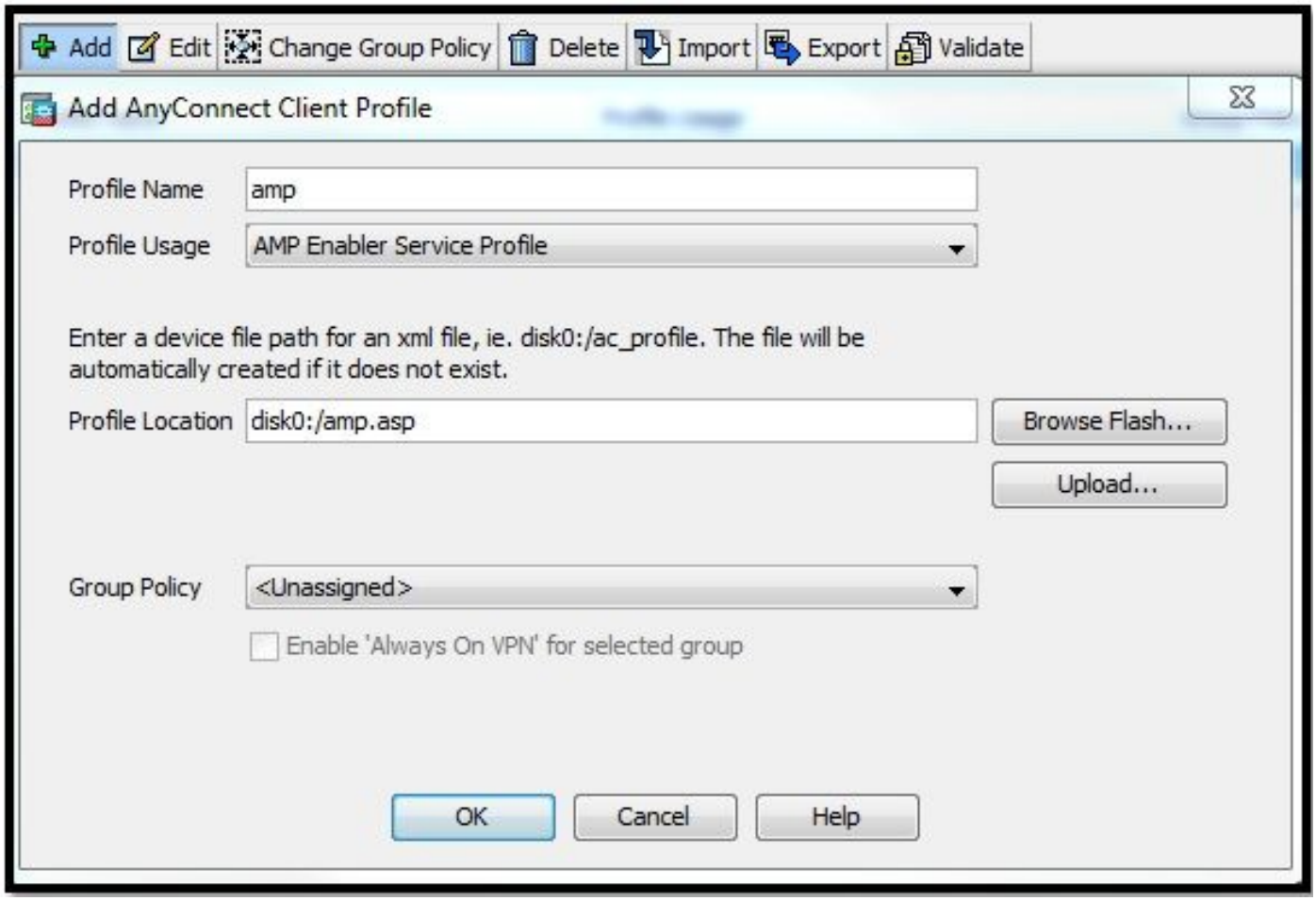
## Implementación de AnyConnect para AMP Enabler a través de ASA

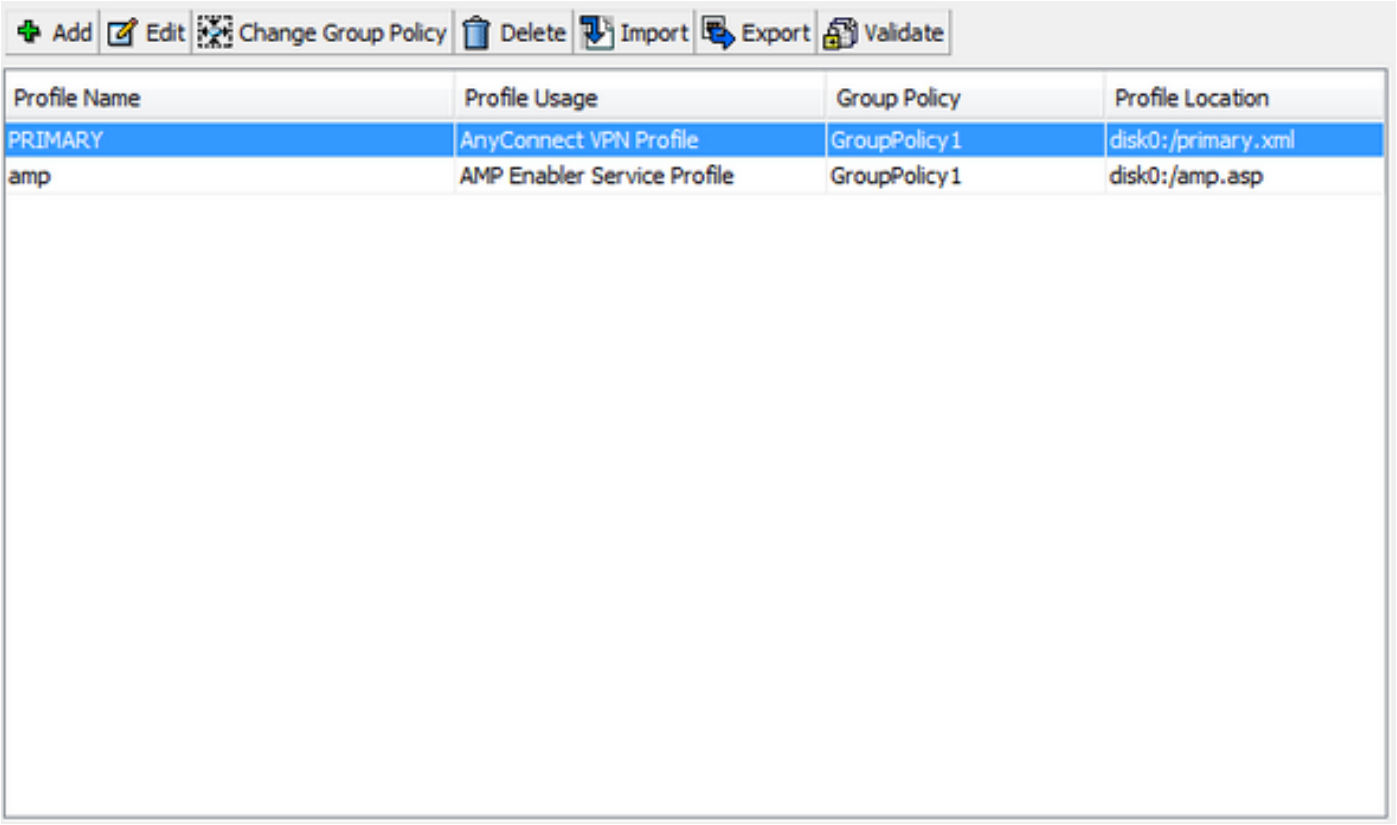
Los pasos involucrados en la configuración son los siguientes:

- Configure el perfil de cliente de AnyConnect AMP Enabler.
- Edite la política del grupo VPN de AnyConnect y descargue el perfil de servicio de AMP Enabler.
- Inicie sesión en el panel AMP para obtener el enlace de descarga de URL del conector.
- Verifique la instalación en el equipo del usuario.

### Paso 1: Configuración del perfil del cliente AnyConnect AMP Enabler

- Vaya a **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Client Profile**.
- Agregue el **perfil de servicio de AMP Enabler**.

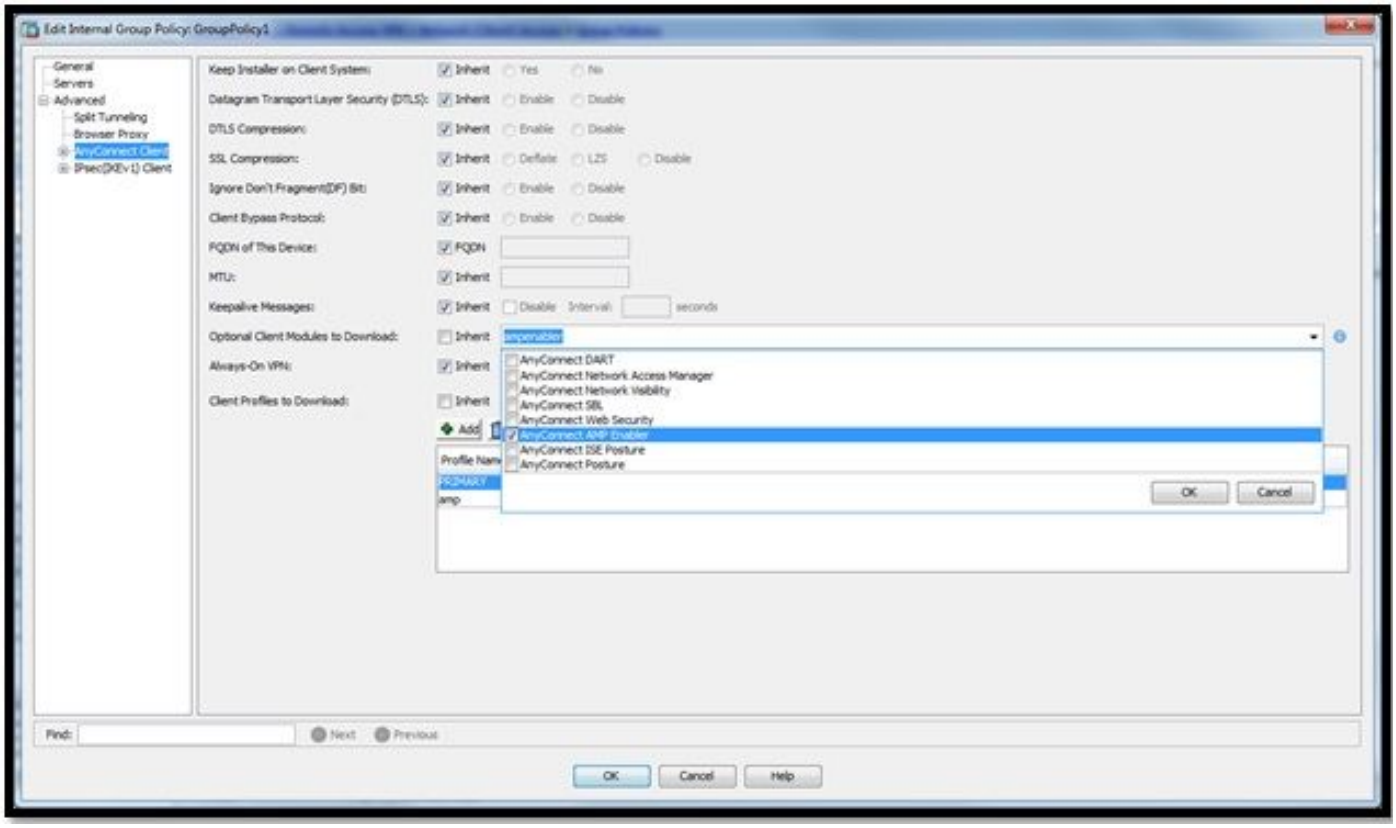



## Paso 2: Editar la política de grupo para descargar el facilitador de AnyConnect AMP

- Vaya a **Configuration > Remove Access VPN > Group Policies > Edit**.
- Vaya a **Advanced > AnyConnect Client > Optional Client Modules to Download.**

- Elija **AnyConnect AMP Enabler.**




## Paso 3: Descargue la política de FireAMP

> **Nota:** Antes de continuar, compruebe si el sistema cumple los requisitos de AMP de terminales con Windows Connector.

### Requisitos del sistema para AMP para terminales Conector de Windows

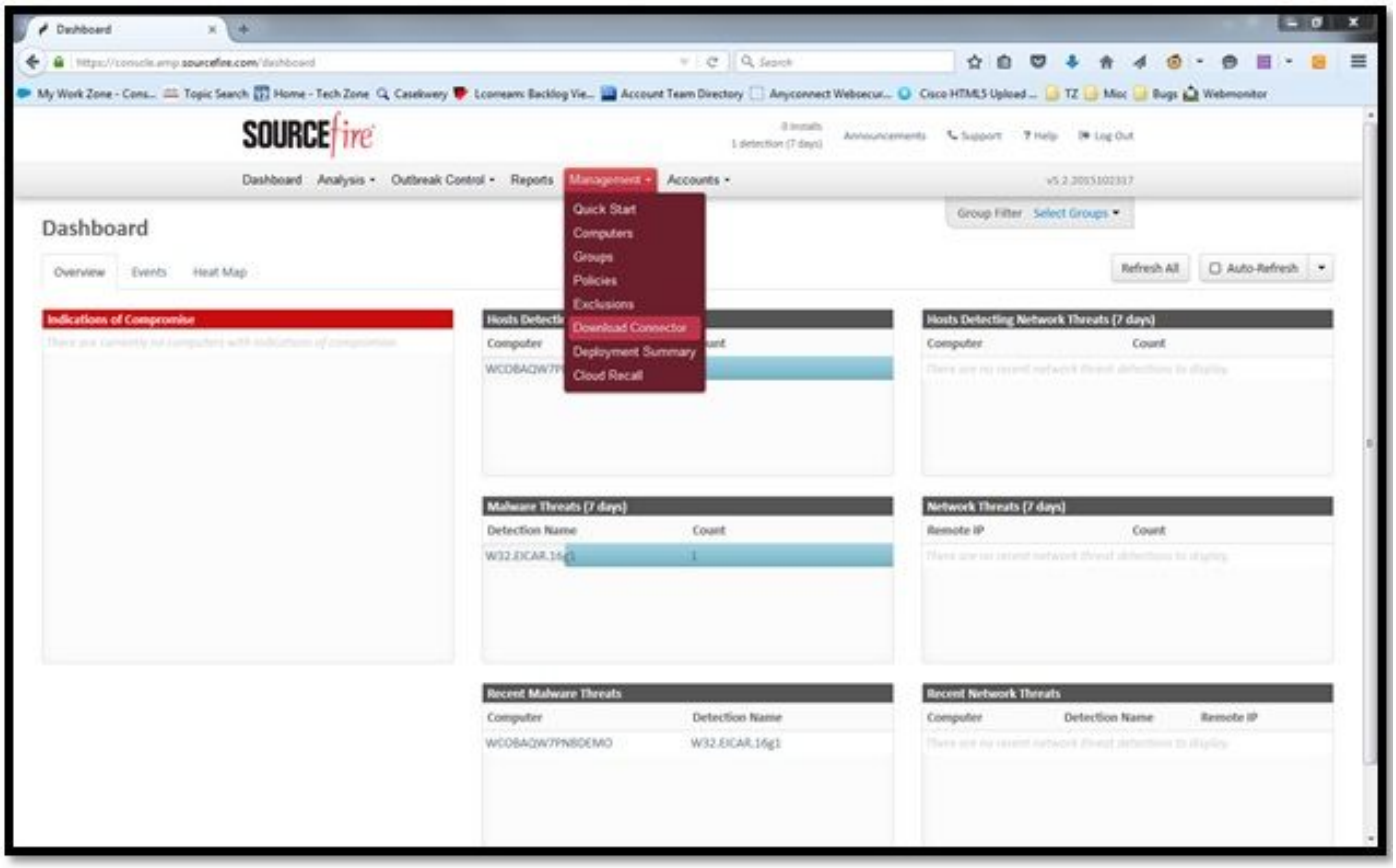
Estos son los requisitos mínimos del sistema para el conector de FireAMP basado en el sistema operativo Windows. El conector FireAMP admite versiones de 32 y 64 bits de estos sistemas operativos. La documentación más reciente de AMP se puede encontrar en la implementación de AMP

| Sistema operativo | Procesador | Memoria | Espacio de disco, Modo sólo nube | Espacio de disco |
|---|---|---|---|---|
| **Microsoft Windows 7** | Procesador de 1 GHz o superior | 1 GB de RAM | 150 MB de espacio disponible en el disco duro - Modo solo en la nube | 1 GB de espacio disponible en disco duro - TETRA |
| **Microsoft Windows 8 y 8.1 (requiere FireAMP Connector 5.1.3 o posterior)** | Procesador de 1 GHz o superior | 512 MB de RAM | 150 MB de espacio disponible en el disco duro - Modo solo en la nube | 1 GB de espacio disponible en disco duro - TETRA |
| **Microsoft** | Procesador de 1 | 512 MB de RAM | 150 MB de | 1 GB de espacio |

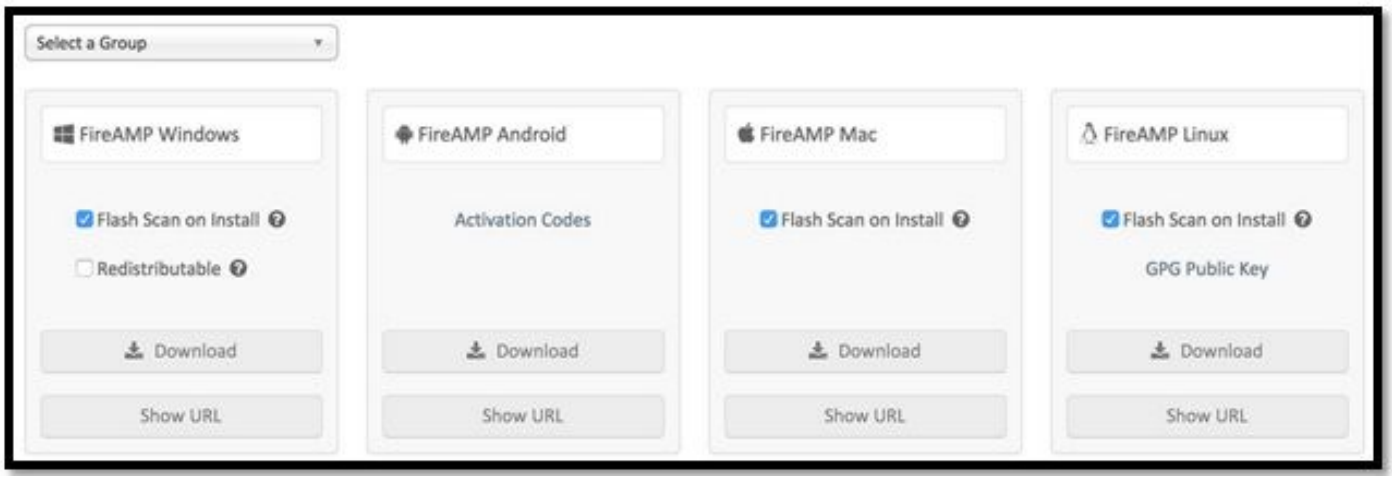
| | | | | |
|---|---|---|---|---|
| **Windows Server 2003** | GHz o superior | | espacio disponible en el disco duro - Modo solo en la nube | disponible en disco duro - TETRA |
| **Microsoft Windows Server 2008** | Procesador de 2 GHz o superior | 2 GB de RAM | 150 MB de espacio de disco duro disponible: modo solo nube | 1 GB de espacio disponible en disco duro - TETRA |
| **Microsoft Windows Server 2012 (requiere FireAMP Connector 5.1.3 o posterior)** | Procesador de 2 GHz o superior | 2 GB de RAM | 150 MB de espacio de disco duro disponible: modo solo nube | Espacio disponible en disco duro de 1 GB - TETRA |

**Lo más común es que el instalador de AMP se coloque en el servidor web de la empresa.**

Para descargar el conector, navegue hasta **Management > Download Connector**. A continuación, elija type y **Download** FireAMP (Windows, Android, Mac, Linux).




La página Download Connector (Descargar conector) le permite descargar los paquetes de instalación para cada tipo de conector FireAMP. Este paquete se puede colocar en un recurso compartido de red o distribuirse a través del software de administración.




### Seleccionar un grupo

- **Sólo auditoría:** Monitoreo del sistema basado en SHA-256 calculado sobre cada archivo. Este modo solo de auditoría no pone en cuarentena el malware, pero envía un evento como alerta.
- **Proteger:** Modo de protección con cuarentena de archivos malintencionados. Supervisar la copia y el movimiento de archivos.
- **Triage:** Esto se utiliza en equipos ya comprometidos/infectados.
- **Servidor:** Conjunto de aplicaciones de instalación para el servidor Windows, donde el conector se instala sin el motor Tetra y el controlador DFC. Este grupo está diseñado por su nombre para servidores de controlador que no son de dominio.
- **Controlador de dominio:** La política predeterminada para este grupo se establece en modo de auditoría como en el grupo Servidor. Asocie todos los servidores de directorio activo de este grupo, lo que significa que el conector se ejecutará en un controlador de dominio de Windows.

AMP tiene la función llamada TETRA, que es un motor antivirus completo. Esta opción es opcional por política.

### Funciones

- **Análisis Flash al instalar:** El proceso de análisis se ejecuta durante la instalación. Su rendimiento es relativamente rápido y se recomienda ejecutarlo sólo una vez.
- **Redistribuible:** Debe descargar un solo paquete, que contiene instaladores de 32 bits y 64 bits. En lugar de un bootstrapper, que está disponible dejando esta opción sin marcar y descargando los archivos del instalador, una vez ejecutado.

> **Nota:** Puede crear su propio grupo y configurar la política asociada. El propósito es colocar todos los servidores de directorio activo, por ejemplo, en un grupo, donde la política está en modo de auditoría.
> El bootstrapper y el instalador redistribuible también contienen un archivo policy.xml que se utiliza como archivo de configuración para el conector AMP.

## Paso 4: Descargue el perfil del cliente de seguridad web

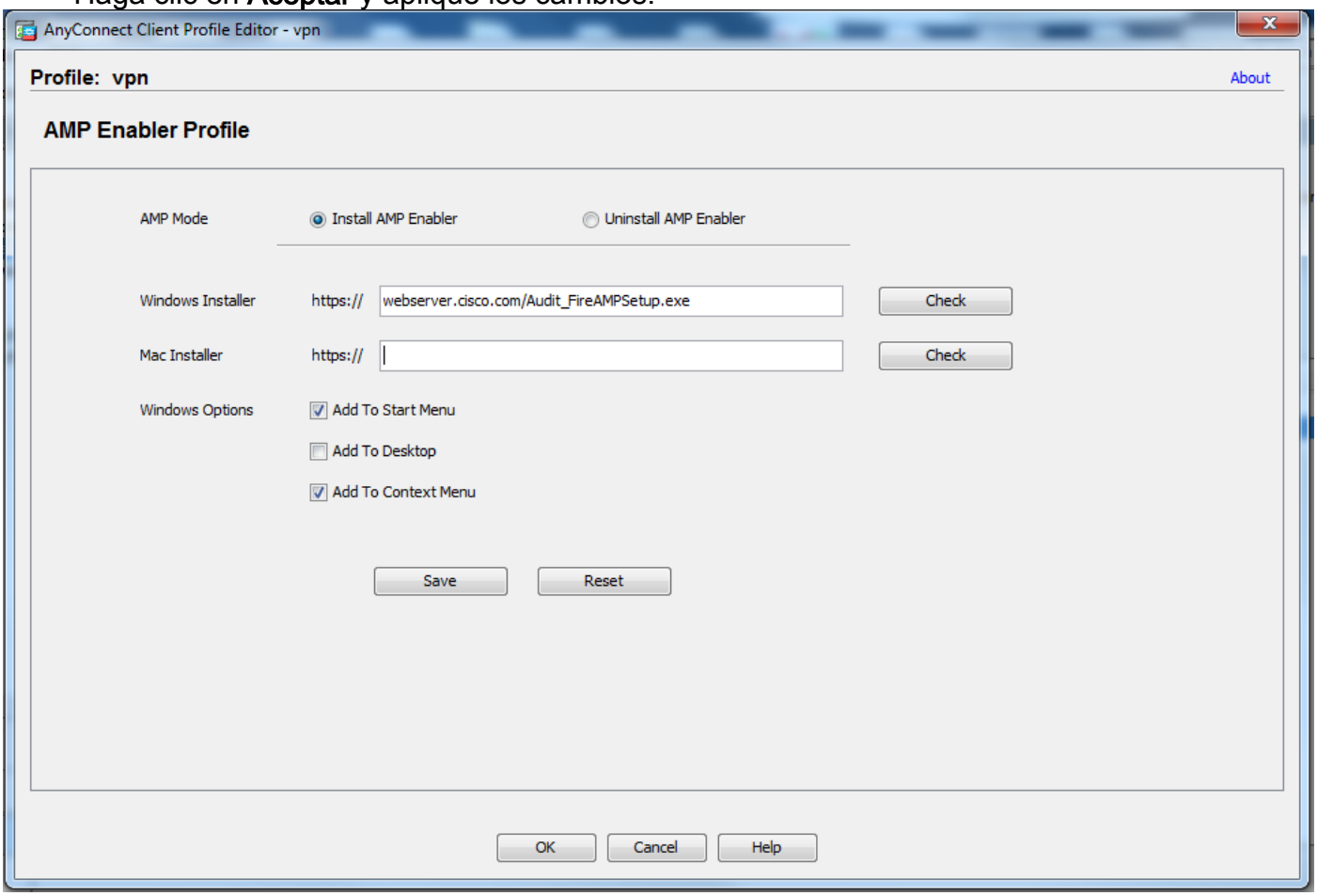
Especifique el servidor web de la empresa o un recurso compartido de red con el instalador de AMP. Esto se utiliza habitualmente en las empresas para ahorrar ancho de banda y colocar instaladores de confianza en una ubicación centralizada.

Asegúrese de que se pueda alcanzar el link HTTPS en los terminales sin ningún error de certificado y que el certificado raíz esté instalado en el almacén de equipos.

Vuelva al perfil de AMP creado anteriormente en el ASA (paso 1) y edite el **perfil de habilitador de AMP**:

1. Para el modo AMP, haga clic en el botón de opción **Install AMP Enabler**.
2. En el campo **Windows Installer**, agregue la IP para el servidor Web y el archivo para FireAMP.
3. Las opciones de Windows son opcionales.

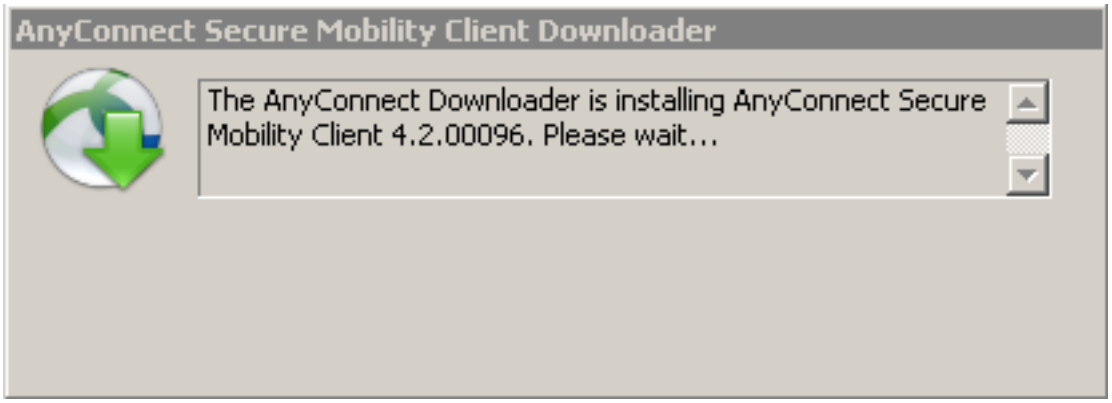
   Haga clic en **Aceptar** y aplique los cambios.




## Paso 5: Conéctese con AnyConnect y verifique la instalación del módulo

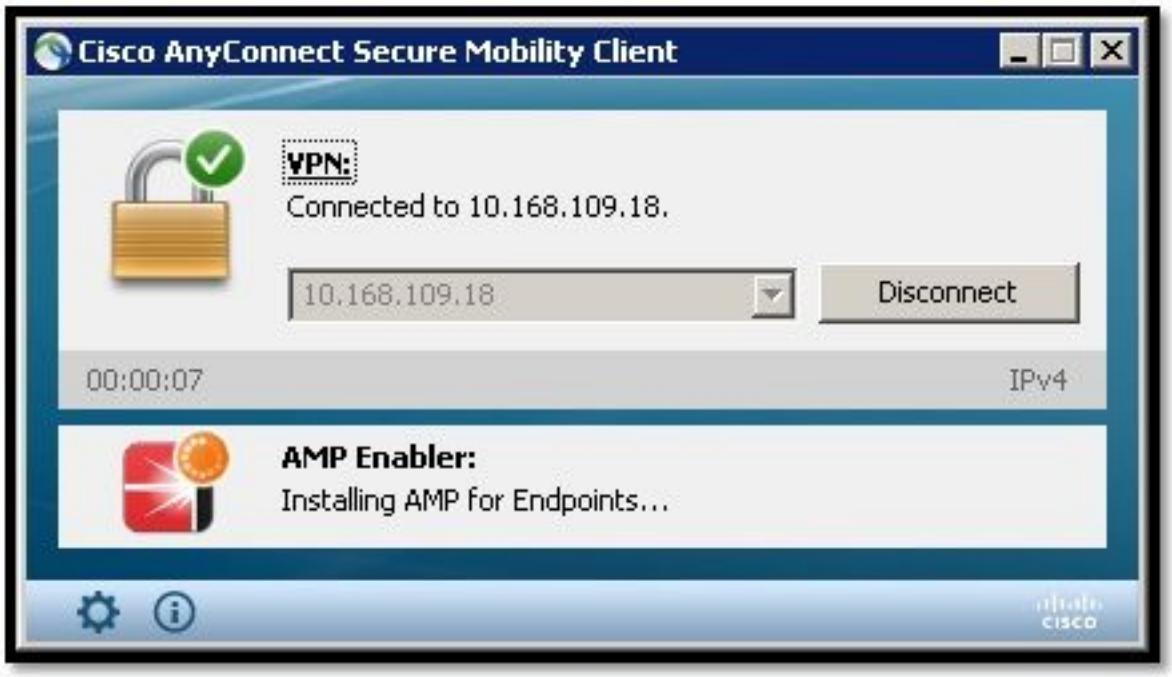
Cuando los usuarios de VPN de Anyconnect se conectan, ASA envía el módulo AnyConnect AMP Enabler a través de la VPN. Para los usuarios que ya han iniciado sesión, se recomienda cerrar la sesión y volver a iniciarla para que se habilite la funcionalidad.

```
10:08:29 AM    Establishing VPN session...
10:08:29 AM    The AnyConnect Downloader is performing update checks...
10:08:29 AM    Checking for profile updates...
10:08:29 AM    Checking for product updates...
10:08:31 AM    Downloading AnyConnect AMP Enabler 4.4.01054 - 48%
10:08:32 AM    Downloading AnyConnect AMP Enabler 4.4.01054 - 91%
10:08:33 AM    Downloading AnyConnect AMP Enabler 4.4.01054 - 100%
```




## Paso 6: Iniciar conexión VPN instalar AMP Enabler y conector AMP

Una vez que pulsa el botón conectar para iniciar la VPN, descarga el nuevo módulo del descargador. Esto tendrá el habilitador de AMP y descargará el paquete de AMP desde la ruta de acceso URL que especificó con un par de pasos antes.




```
If you look at the event viewer:

AMP enabler install:
Date         : 04/24/2017
Time         : 10:08:34
Type         : Information
Source       : acvpndownloader

Description : Cisco AnyConnect Secure Mobility Client Downloader (2) exiting, version 4.4.01054
, return code 0 [0x00000000]
```

## Paso 7: Verifique AnyConnect y verifique si todo está instalado

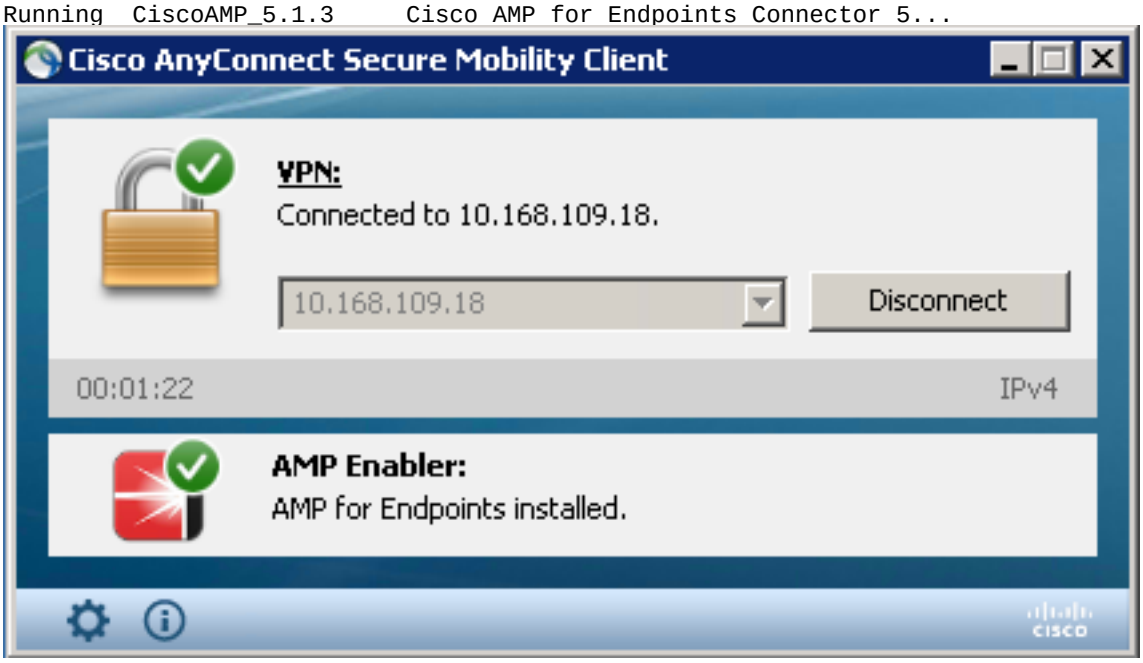
Una vez que la VPN esté conectada y la configuración del servidor web esté instalada, verifique AnyConnect y verifique que todo esté instalado correctamente.

En services.msc puede encontrar un nuevo servicio llamado CiscoAMP_5.1.3. En el comando

PowerShell vemos:

```
PS C:\Users\winUser348> Get-Service -name "*CiscoAMP*"

Status   Name               DisplayName
------   ----               -----------
Running  CiscoAMP_5.1.3     Cisco AMP for Endpoints Connector 5...
```




El instalador de AMP agrega nuevos controladores al sistema operativo Windows. Puede utilizar el comando driverquery para enumerar los controladores.

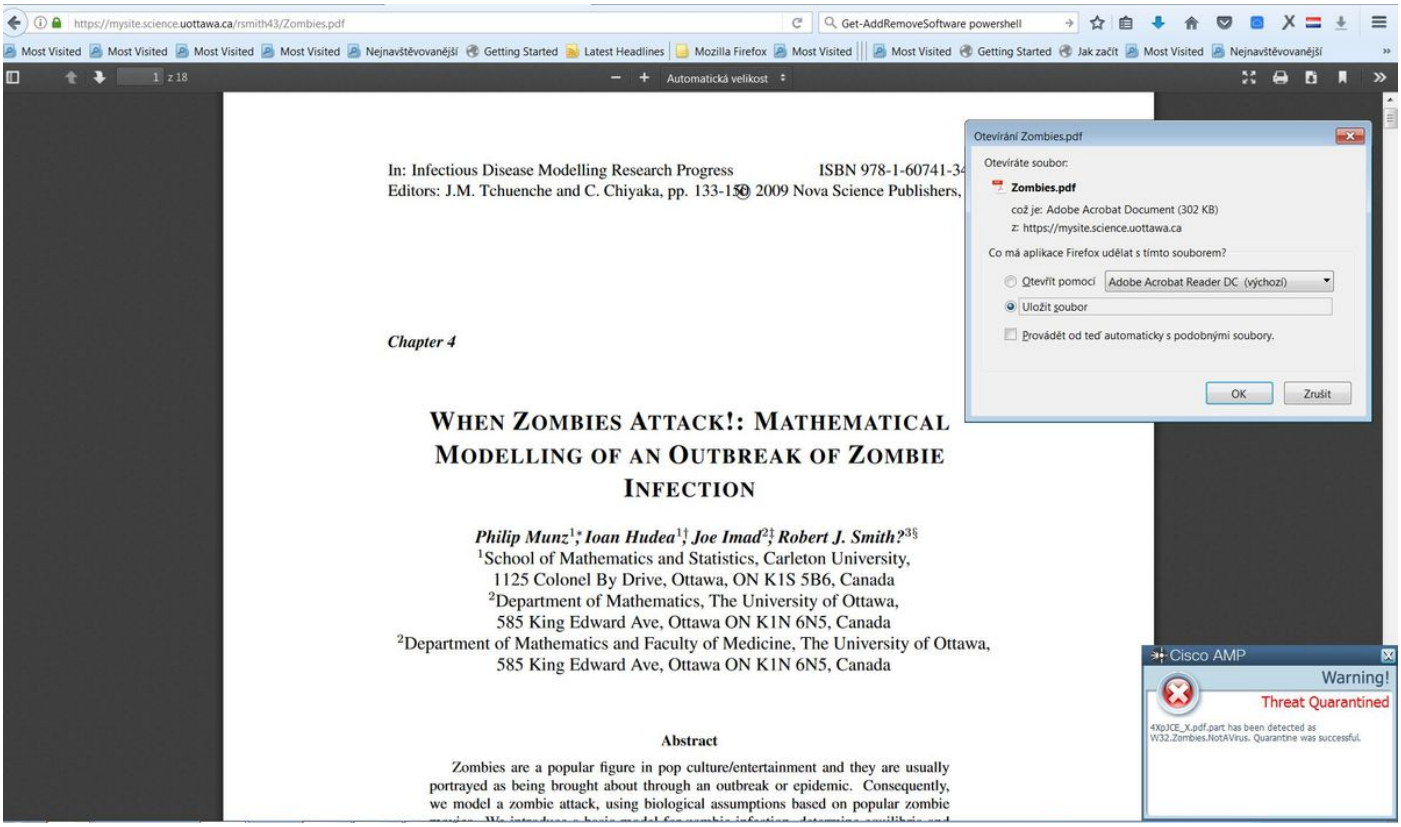
```
C:\Windows\System32>driverquery /v | findstr immunet

ImmunetProte ImmunetProtectDriver   ImmunetProtectDriver   File System   System     Running
OK           TRUE         FA
LSE          4,096       69,632      0       3/17/2017 5:04:20 PM
\??\C:\WINDOWS\System32\Drivers\immunetprotect.s 8,192

ImmunetSelfP ImmunetSelfProtectDriv ImmunetSelfProtectDriv File System   System     Running
OK           TRUE         FA
LSE          4,096       28,672      0       3/17/2017 5:04:08 PM
\??\C:\WINDOWS\System32\Drivers\immunetselfprote 8,192
```

## Paso 8: Prueba con una cadena Eicar contenida en un archivo PDF de Zombies

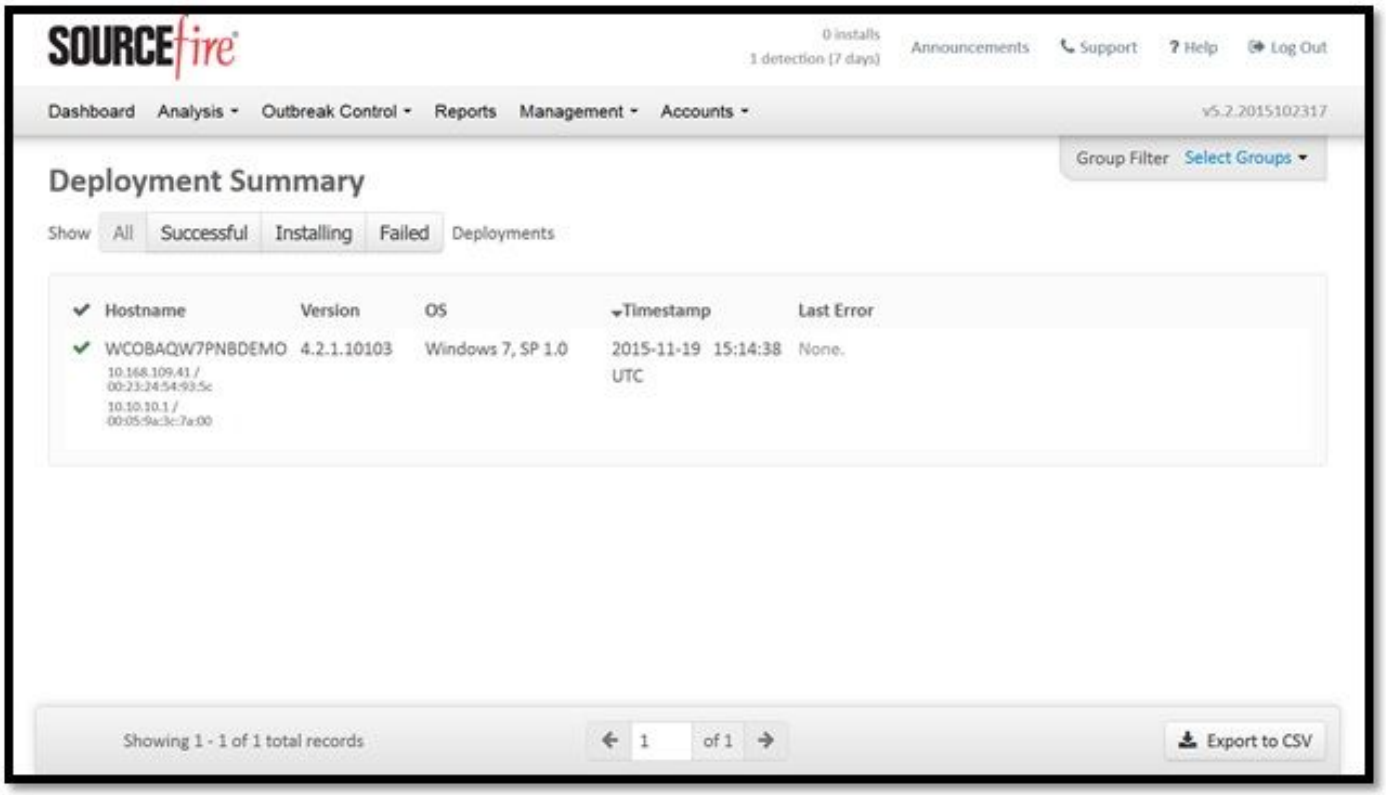
Pruebe con una cadena Eicar contenida en un archivo PDF de Zombies en un equipo de prueba para verificar que el archivo malicioso está en cuarentena.




Zombies.pdf contiene la cadena Eicar

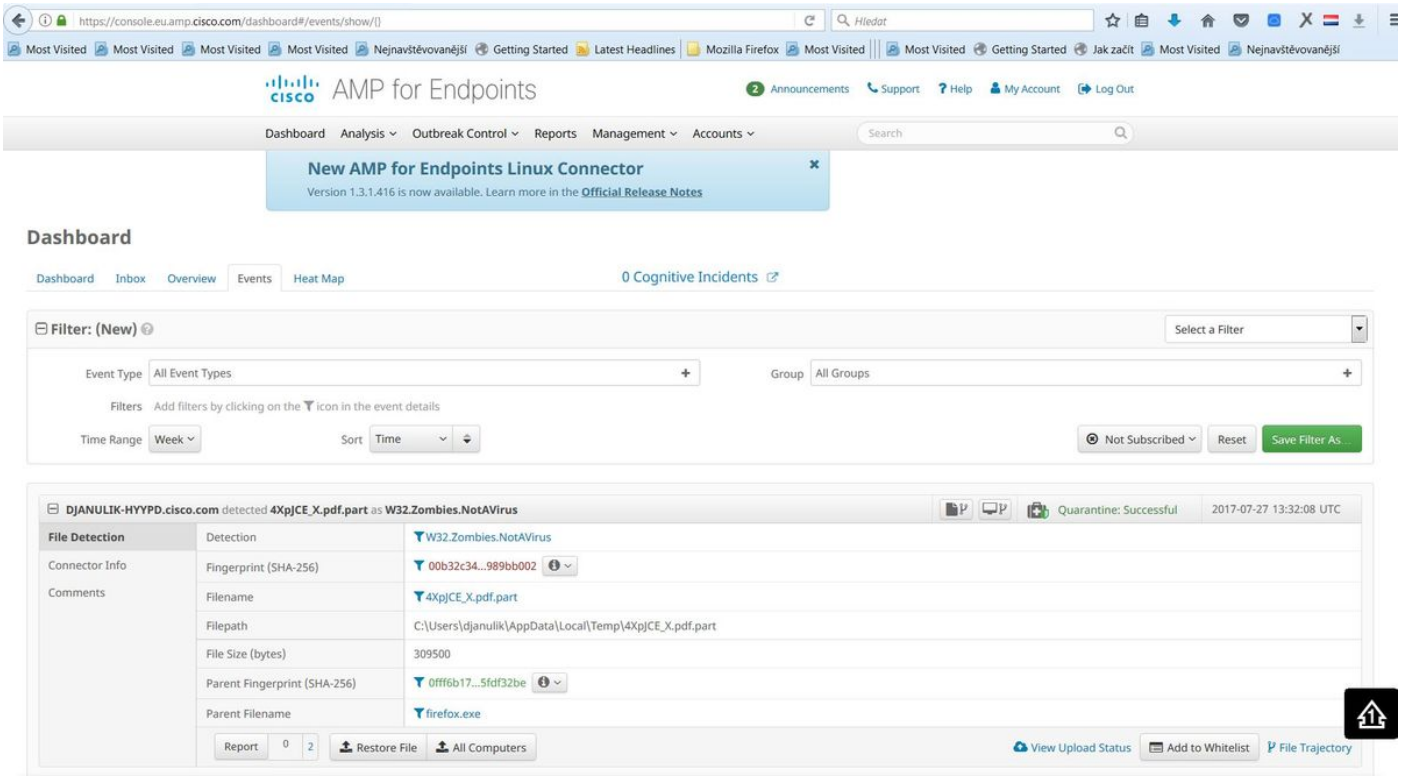
## Paso 9: Resumen de la implementación

En esta página se muestra una lista de las instalaciones del conector FireAMP que han fallado y se han realizado correctamente, así como de las que se encuentran en curso. Puede ir a **Administración > Resumen de implementación**.




## Paso 10: Verificación de detección de subprocesos

Zombies.pdf desencadenó un evento de cuarentena y lo envió al panel de AMP.



Evento de cuarentena

# Additional Information

Para obtener su cuenta de AMP, puede inscribirse en la ATS University. Esto le ofrece una descripción general de la funcionalidad de AMP en LAB.

# Información Relacionada

- Configuración de AMP Enabler
- Soporte Técnico y Documentación - Cisco Systems