Installation and Configuration of AMP Module Through AnyConnect 4.x and AMP Enabler

Contents

Introduction

This document goes through steps to install the Advanced Malware Protection (AMP) connector with AnyConnect.

The AnyConnect AMP Enabler is used as a medium to deploy AMP for Endpoints. Itself it does not have any capability to convict file disposition. It pushes the AMP for Endpoints software to an endpoint from ASA. Once the AMP is installed it uses cloud capacity to check for files disposition. Further AMP service can submit files to dynamic analysis called ThreatGrid, to score unknown files behaviour. These files can be convicted as malicious if certain artifacts are met. This is widely usefull for zero-day attacks.

Prerequisites

Requirements

- AnyConnect Secure Mobility Client Version 4.x
- FireAMP / AMP for Endpoints
- Adaptive Security Device Manager (ASDM) Version 7.3.2 or later

Components Used

The information in this document is based on these software and hardware versions:

- Adaptive Security Appliance (ASA) 5525 with Software Version 9.5.1
- AnyConnect Secure Mobility Client 4.2.00096 on Microsoft Windows 7 Professional 64-bit
- ASDM Version 7.5.1(112)

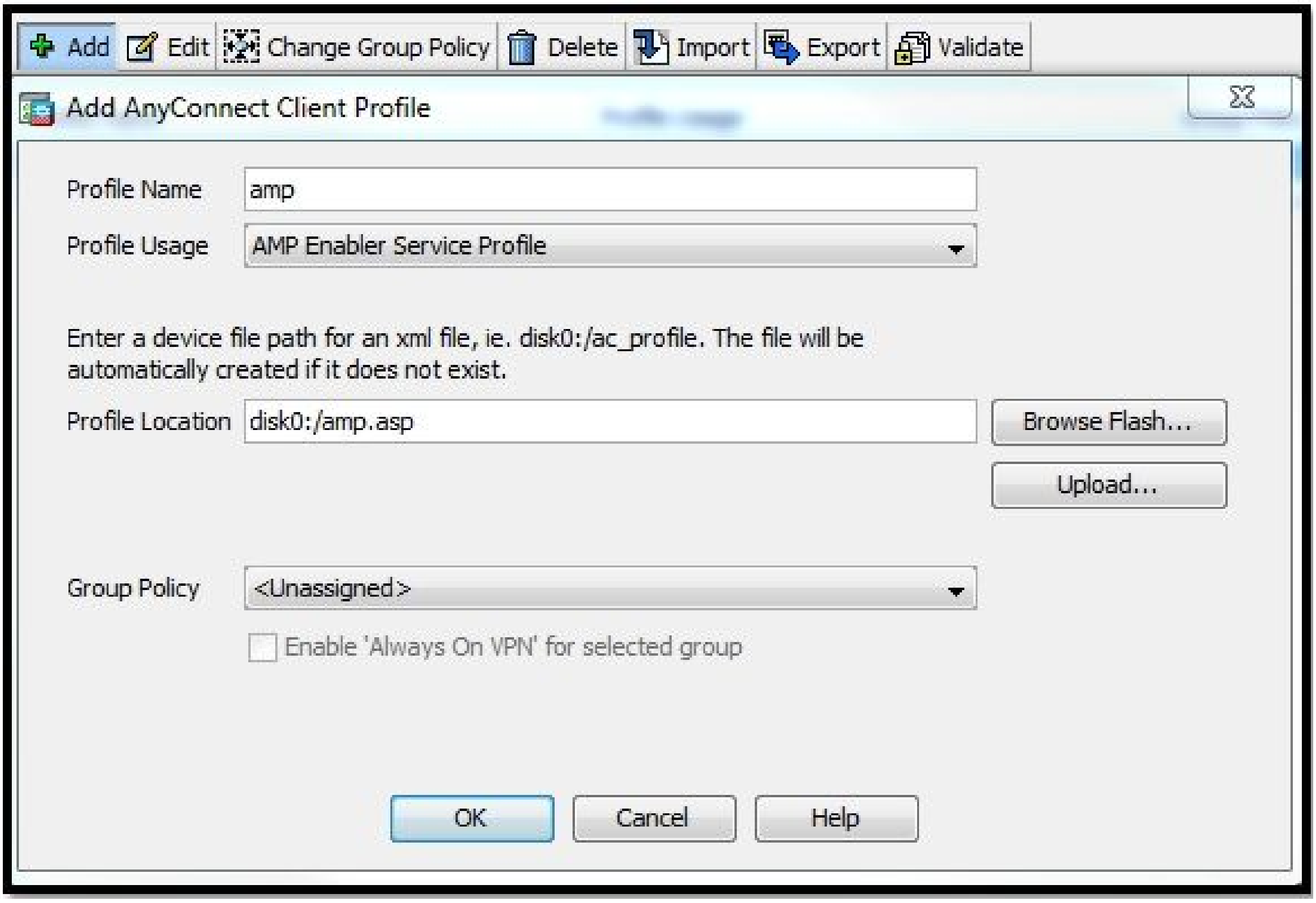
AnyConnect Deployment for AMP Enabler through ASA

The steps involved in the configuration are as follows:

- Configure the AnyConnect AMP Enabler client profile.
- Edit the AnyConnect VPN group policy and download the AMP Enabler Service Profile.
- Login to the AMP dashboard in order to get the connector URL download link.
- Verify the installation on the user machine.

Step 1: Configure the AnyConnect AMP Enabler Client Profile

- Navigate to **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Client Profile**.
- Add the **AMP Enabler Service Profile**.



Add AnyConnect Client Profile

Profile Name: amp

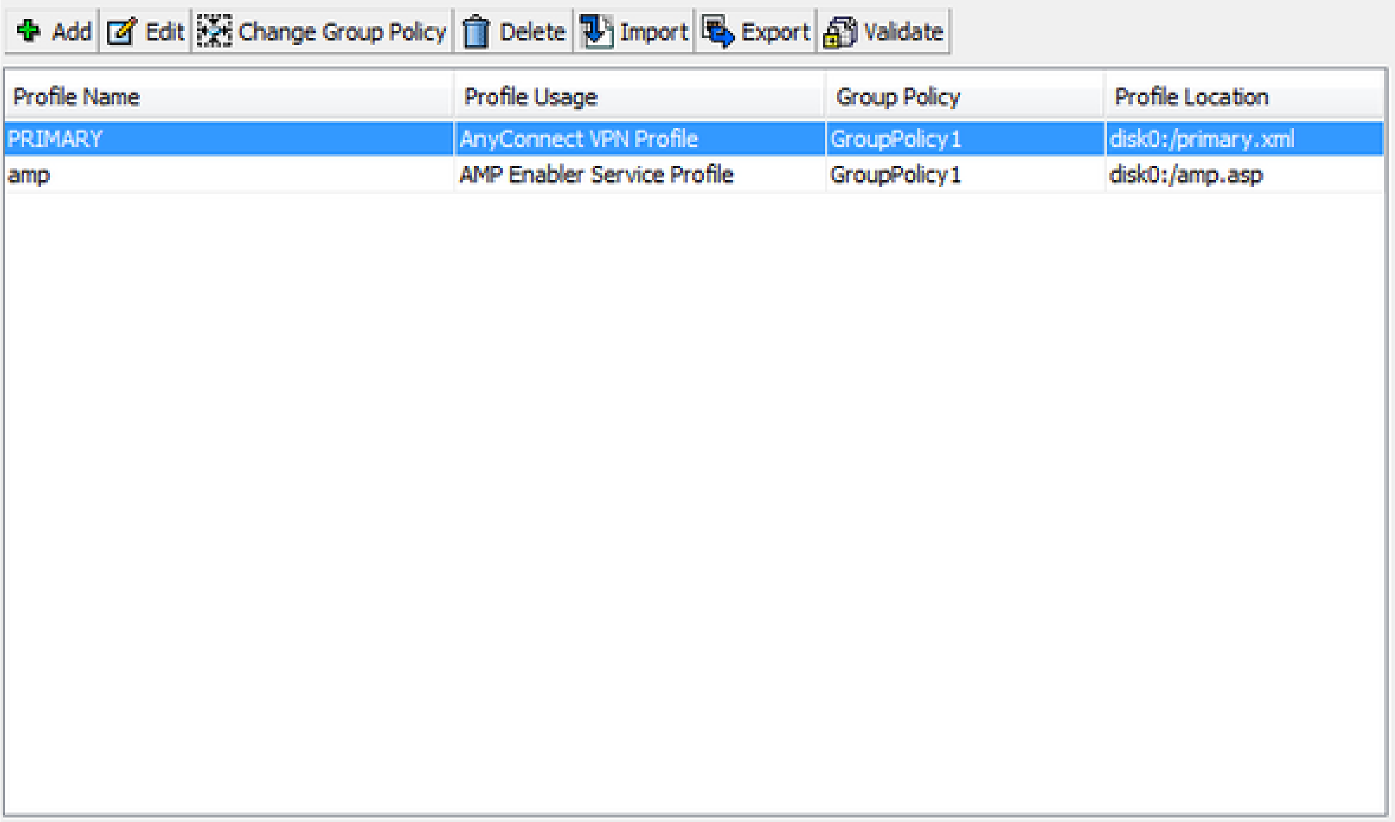
Profile Usage: AMP Enabler Service Profile

Enter a device file path for an xml file, ie. disk0:/ac_profile. The file will be automatically created if it does not exist.

Profile Location: disk0:/amp.asp

Group Policy: <Unassigned>

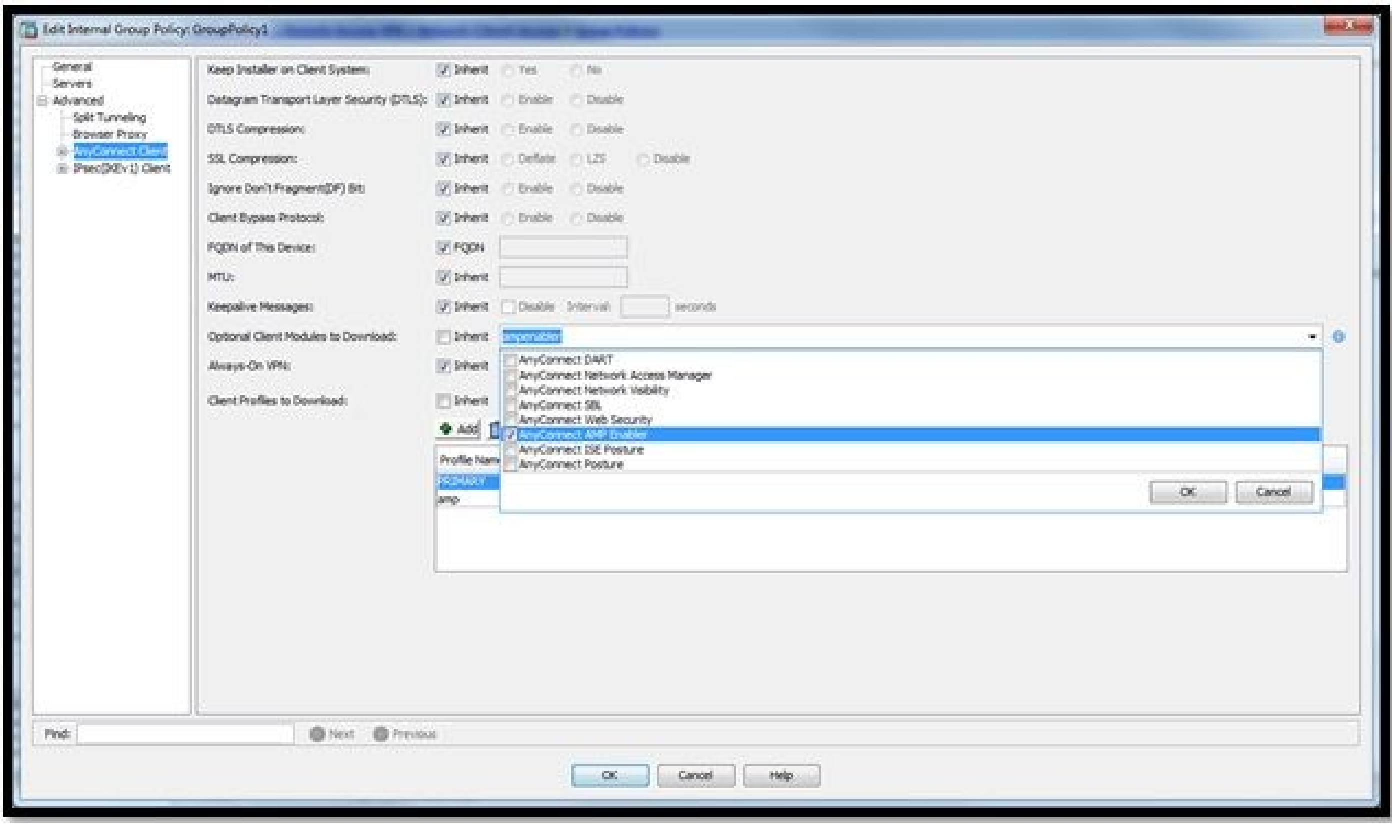
□ Enable 'Always On VPN' for selected group



Profile Name	Profile Usage	Group Policy	Profile Location
PRIMARY	AnyConnect VPN Profile	GroupPolicy1	disk0:/primary.xml
amp	AMP Enabler Service Profile	GroupPolicy1	disk0:/amp.asp

Step 2: Edit the Group-Policy to Download the AnyConnect AMP Enabler

- Navigate to **Configuration > Remove Access VPN > Group Policies > Edit**.
- Go to **Advanced > AnyConnect Client > Optional Client Modules to Download.**
- Choose **AnyConnect AMP Enabler.**



Keep Installer on Client System: ☑ Inherit ○ Yes ○ No

Datagram Transport Layer Security (DTLS): ☑ Inherit ○ Enable ○ Disable

DTLS Compression: ☑ Inherit ○ Enable ○ Disable

SSL Compression: ☑ Inherit ○ Deflate ○ LZS ○ Disable

Ignore Don't Fragment(DF) Bit: ☑ Inherit ○ Enable ○ Disable

Client Bypass Protocol: ☑ Inherit ○ Enable ○ Disable

FQDN of This Device: ☑ FQDN

MTU: ☑ Inherit

Keepalive Messages: ☑ Inherit □ Disable Interval: seconds

Optional Client Modules to Download: □ Inherit ampenabler

- □ AnyConnect DART
- □ AnyConnect Network Access Manager
- □ AnyConnect Network Visibility
- □ AnyConnect SBL
- □ AnyConnect Web Security
- ☑ AnyConnect AMP Enabler
- □ AnyConnect ISE Posture
- □ AnyConnect Posture

Always-On VPN: ☑ Inherit

Client Profiles to Download: □ Inherit

Profile Name
PRIMARY
amp

Step 3: Download the FireAMP Policy

Note: Before you proceed, check if your system meets the requirements for the AMP of Endpoints Windows Connector.

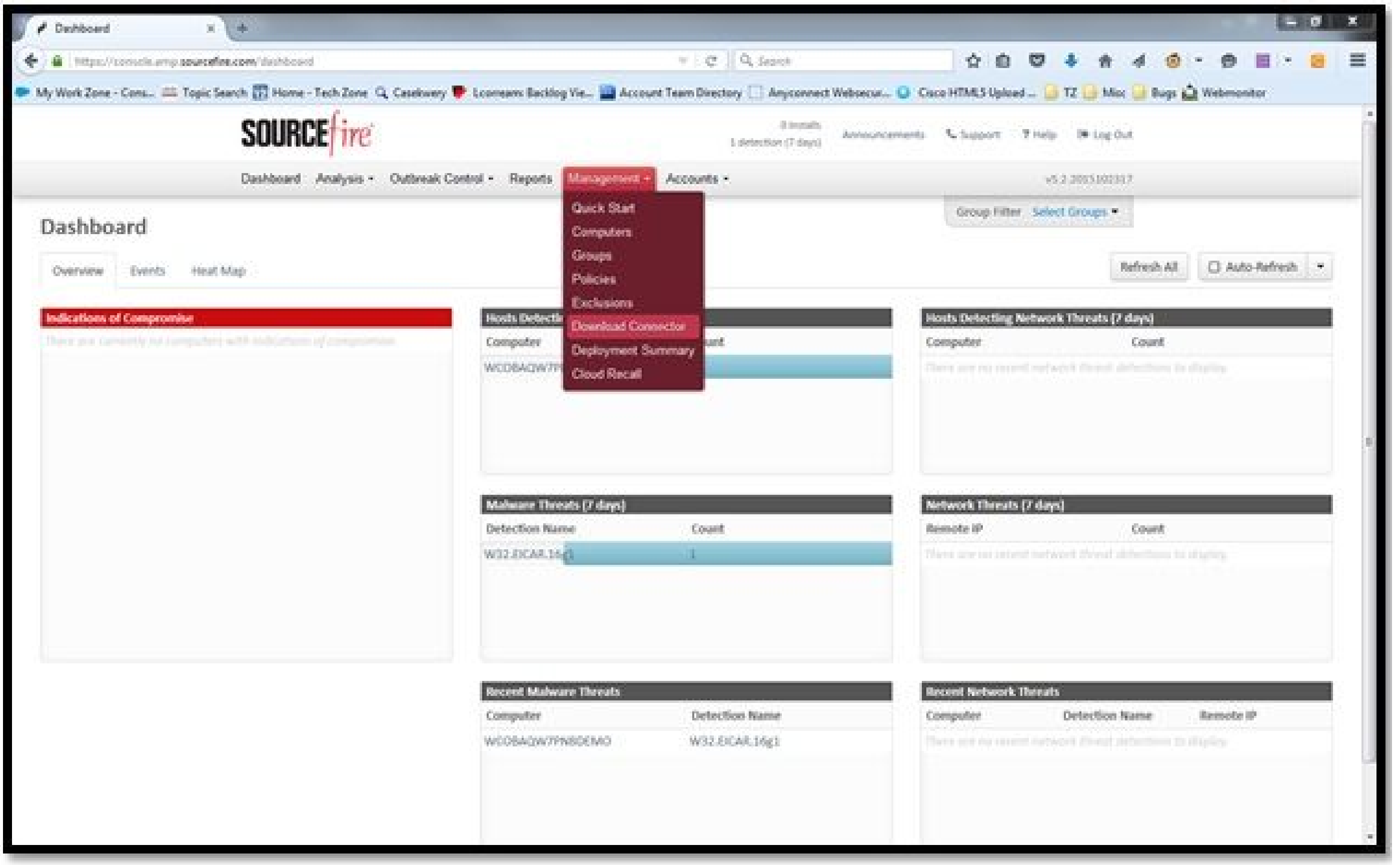
System Requirements for AMP for Endpoints Windows Connector

These are the minimum system requirements for the FireAMP Connector based on the Windows operating system. The FireAMP Connector supports both 32-bit and 64-bit versions of these operating systems. The latest AMP documentation can be found in AMP deployment

Operating System	Processor	Memory	Disk Space, Cloud Only Mode	Disk Space
Microsoft Windows 7	1 GHz or faster processor	1 GB RAM	150 MB available hard disk space - Cloud-only mode	1GB available hard disk space - TETRA
Microsoft Windows 8 and 8.1 (requires FireAMP Connector 5.1.3 or later)	1 GHz or faster processor	512 MB RAM	150 MB available hard disk space - Cloud-only mode	1GB available hard disk space – TETRA
Microsoft Windows Server 2003	1 GHz or faster processor	512 MB RAM	150 MB available hard disk space - Cloud-only mode	1GB available hard disk space - TETRA
Microsoft Windows Server 2008	2 GHz or faster processor	2 GB RAM	150 MB available hard disk space – Cloud only mode	1GB available hard disk space – TETRA
Microsoft Windows Server 2012 (requires FireAMP Connector 5.1.3 or later)	2 GHz or faster processor	2 GB RAM	150 MB available hard disk space - Cloud only mode	1 GB available hard disk space – TETRA

Most common is to have the AMP installer placed on the enterprise web server.

In order to download the connector, navigate to **Management > Download Connector**. Then choose type, and **Download** FireAMP (Windows, Android, Mac, Linux).



Dashboard

Indications of Compromise

There are currently no computers with indications of compromise.

Hosts Detecting Network Threats (7 days)

Computer	Count
There are no recent network threat detections to display.	

Malware Threats (7 days)

Detection Name	Count
W32.EICAR.16g1	1

Network Threats (7 days)

Remote IP	Count
There are no recent network threat detections to display.	

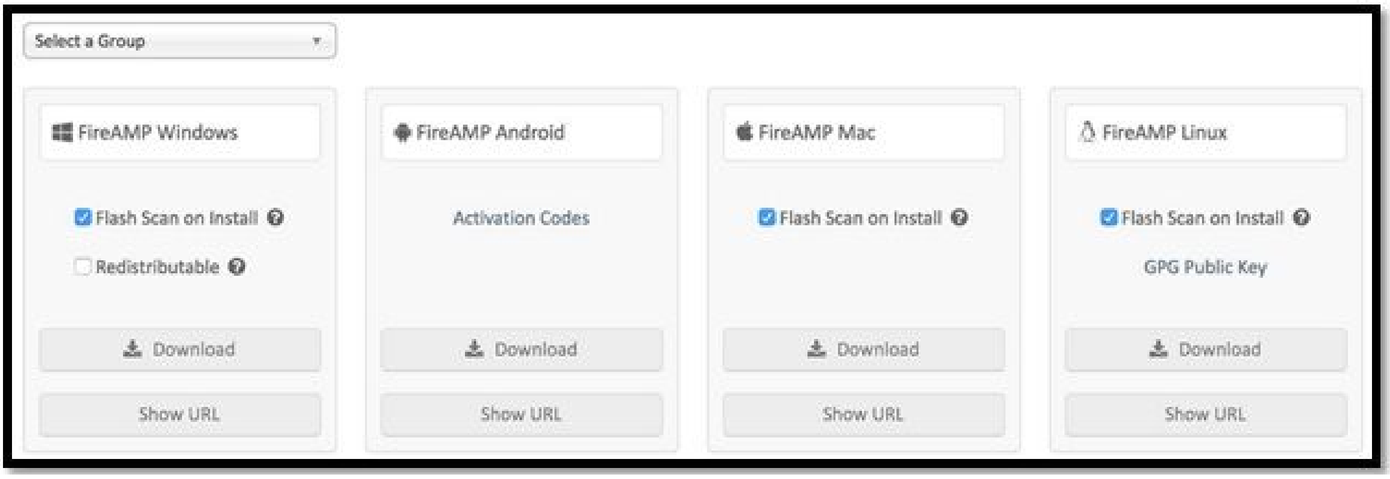
Recent Malware Threats

Computer	Detection Name
WCDBAQW7PN8DEMO	W32.EICAR.16g1

Recent Network Threats

Computer	Detection Name	Remote IP
There are no recent network threat detections to display.		

The Download Connector page allows you to download the install packages for each type of FireAMP connector. This package can be placed on a network share or distributed via management software.



Select a Group

- **Audit Only:** Monitoring the system based on SHA-256 calculated over each file. This Audit only mode does not quarantine the malware, but sends an event as an alert.
- **Protect:** Protect mode with quarantine malicious files. Monitor file copy and move.
- **Triage:** This is for use on already compromised/infected computer.
- **Server:** Installation suite for Windows server, where the connector installs without Tetra engine and DFC driver. This group is designed by its name for non-domain controller servers.
- **Domain Controller:** The default policy for this group is set to audit mode as in Server group. Associate all your Active directory servers in this group, that means the connector will be running on a Windows Domain Controller.

The AMP has the feature called TETRA, which is full antivirus engine. This option is optional per policy.

Features

- **Flash Scan on Install:** Scan process runs during the installation. It is relatively quick to perform and recommended to run only once.
- **Redistributable:** You should download one single package, which contains 32-bit and 64-bit installers. Rather than a bootstrapper, which is available leaving this option unticked and downloads the installer files, once executed.

> **Note**: You can create your own group and configure associated policy to it. The purpose is to place all e.g. Active directory servers into one group, where the policy is in audit mode.
> The bootstrapper and redistributable installer also both contain a `policy.xml` file that is used as a configuration file for the AMP connector.

Step 4: Download the Web Security Client Profile

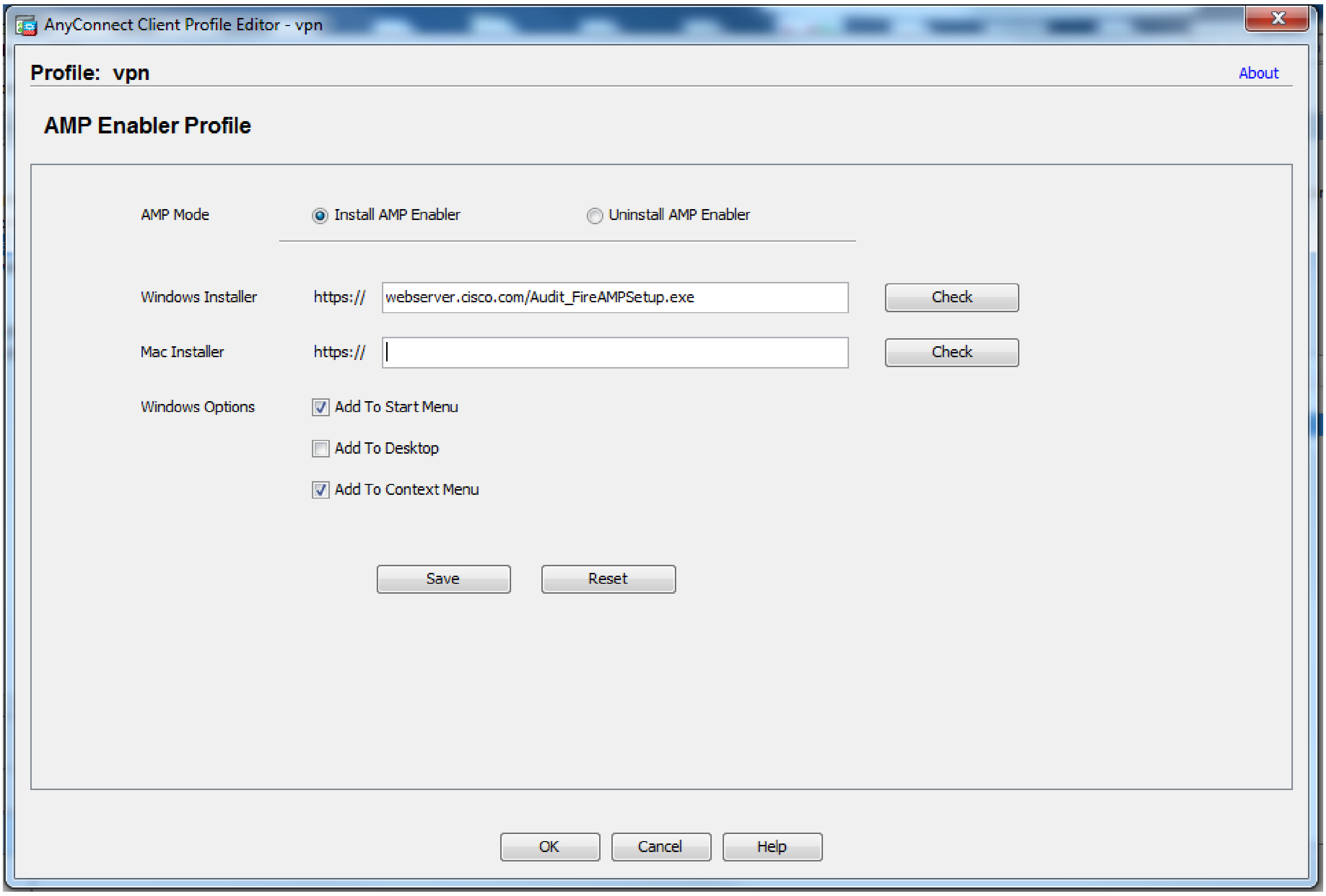
Specify company web server or a network share with AMP installer. This is most commonly used across companies to save bandwidth and place trusted installers in centralized location.

Please be sure that the HTTPS link can be reached on the endpoints without any certificate error and that root certificate is installed in the machine store.

Go back to the AMP Profile created before on the ASA (step 1) and edit **AMP Enabler Profile**:

1. For AMP Mode, click the **Install AMP Enabler** radio button.
2. In the **Windows Installer** field, add the IP for the web server and the file for the FireAMP.
3. Windows Options are optional.

   Click **OK** and apply the changes.



Profile: vpn

AMP Enabler Profile

AMP Mode ● Install AMP Enabler ○ Uninstall AMP Enabler

Windows Installer https:// webserver.cisco.com/Audit_FireAMPSetup.exe

Mac Installer https://

Windows Options ☑ Add To Start Menu

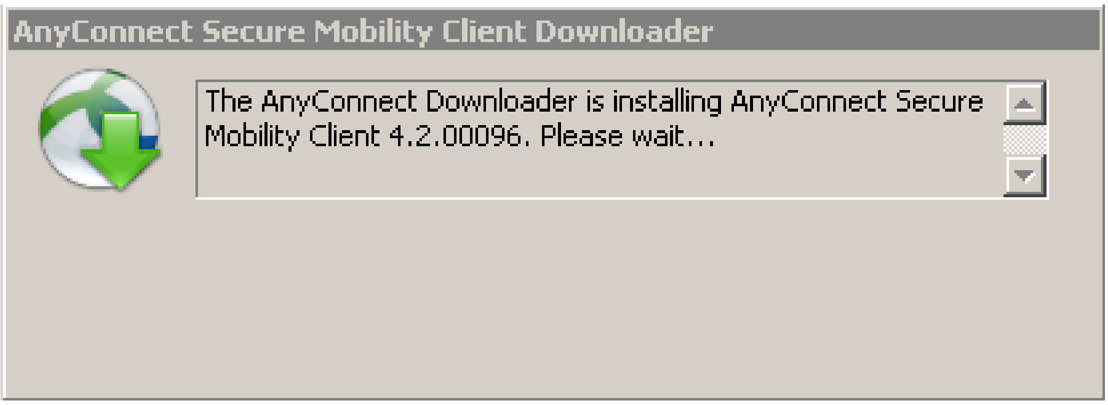
□ Add To Desktop

☑ Add To Context Menu

Step 5: Connect with AnyConnect and Verify the Installation of the Module

When Anyconnect VPN users connect, ASA pushes the AnyConnect AMP Enabler module through the VPN. For already logged in users, it is recommended to log off and then log in back for the functionality to be enabled.

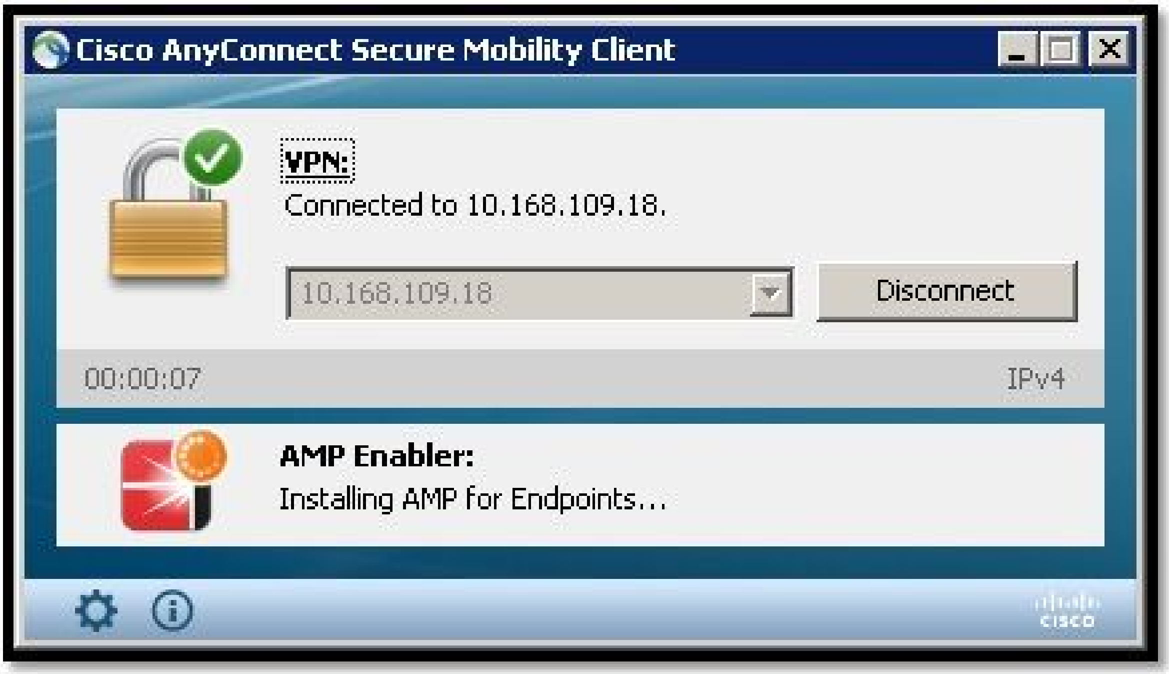
```
10:08:29 AM    Establishing VPN session...
10:08:29 AM    The AnyConnect Downloader is performing update checks...
10:08:29 AM    Checking for profile updates...
10:08:29 AM    Checking for product updates...
10:08:31 AM    Downloading AnyConnect AMP Enabler 4.4.01054 - 48%
10:08:32 AM    Downloading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



The AnyConnect Downloader is installing AnyConnect Secure Mobility Client 4.2.00096. Please wait...

Step 6: Start VPN Connection install AMP Enabler and AMP connector

Once you hit the button connect to start the VPN, it downloads the new downloader module. This will have AMP enabler and downloads the AMP package from the URL path you specified couple of steps before.



Cisco AnyConnect Secure Mobility Client

VPN:
Connected to 10.168.109.18.

AMP Enabler:
Installing AMP for Endpoints...

```
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]
```

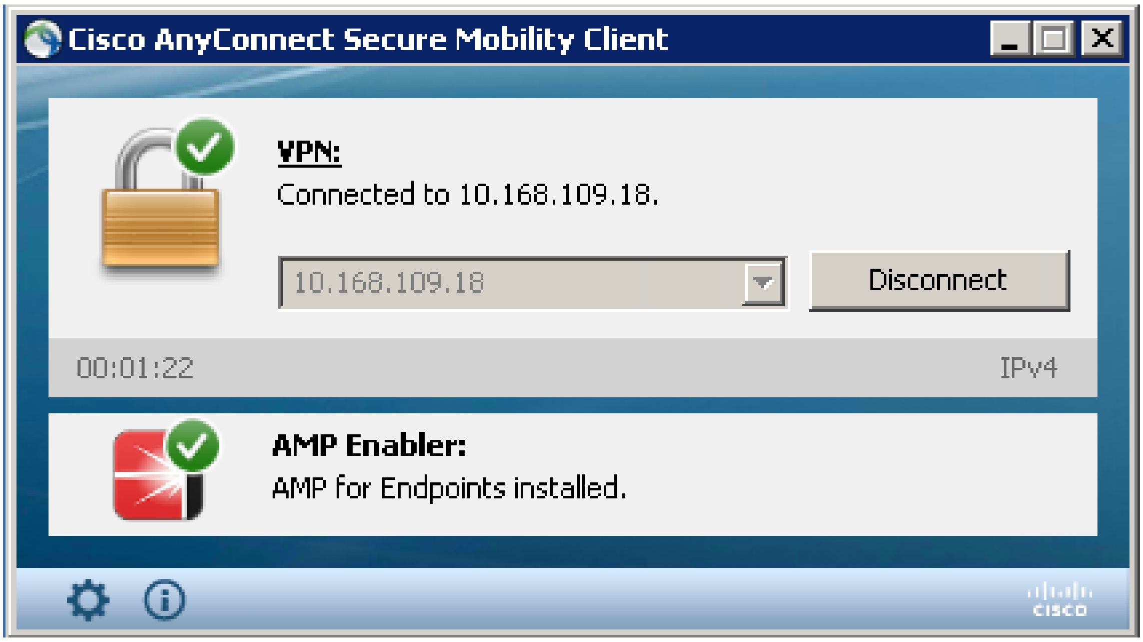
Step 7: Check AnyConnect and Verify If Everything is Installed

Once the VPN is connected and the configuration of the web server is installed, check AnyConnect and verify everything is installed properly.

In the services.msc you can find a new service called CiscoAMP_5.1.3. In the Powershell command we see:

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

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



Connected to 10.168.109.18.

10.168.109.18

00:01:22

IPv4

AMP for Endpoints installed.

The AMP Installer adds new drivers to the Windows OS. You might use the driverquery command to list the dirvers.

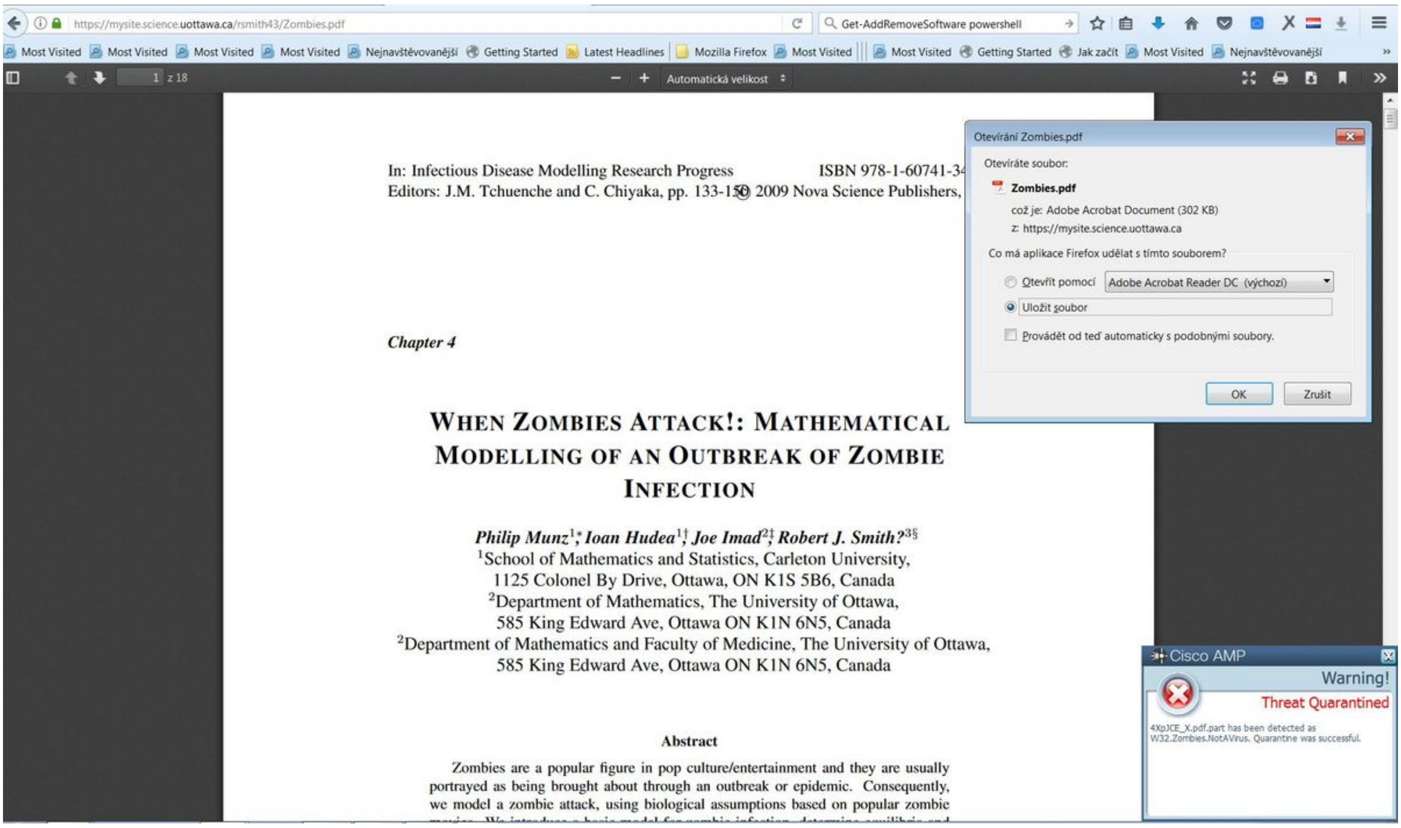
```
C:\Windows\System32>driverquery /v | findstr immunet

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
```

Step 8: Test with an Eicar String Contained in a Zombies PDF File

Test with an Eicar string contained in a Zombies PDF file in a test computer in order to verify the malicious file is quarantined.



In: Infectious Disease Modelling Research Progress ISBN 978-1-60741-34
Editors: J.M. Tchuenche and C. Chiyaka, pp. 133-150 © 2009 Nova Science Publishers,

Chapter 4

WHEN ZOMBIES ATTACK!: MATHEMATICAL MODELLING OF AN OUTBREAK OF ZOMBIE INFECTION

Philip Munz[1]*, *Ioan Hudea*[1]*, *Joe Imad*[2]*, *Robert J. Smith?*[3]
[1]School of Mathematics and Statistics, Carleton University,
1125 Colonel By Drive, Ottawa, ON K1S 5B6, Canada
[2]Department of Mathematics, The University of Ottawa,
585 King Edward Ave, Ottawa ON K1N 6N5, Canada
[2]Department of Mathematics and Faculty of Medicine, The University of Ottawa,
585 King Edward Ave, Ottawa ON K1N 6N5, Canada

Abstract

Zombies are a popular figure in pop culture/entertainment and they are usually portrayed as being brought about through an outbreak or epidemic. Consequently, we model a zombie attack, using biological assumptions based on popular zombie

Otevírání Zombies.pdf

Otevíráte soubor:

Zombies.pdf

což je: Adobe Acrobat Document (302 KB)

z: https://mysite.science.uottawa.ca

Co má aplikace Firefox udělat s tímto souborem?

○ Otevřít pomocí Adobe Acrobat Reader DC (výchozí)

● Uložit soubor

□ Provádět od teď automaticky s podobnými soubory.

OK Zrušit

Cisco AMP

Warning!

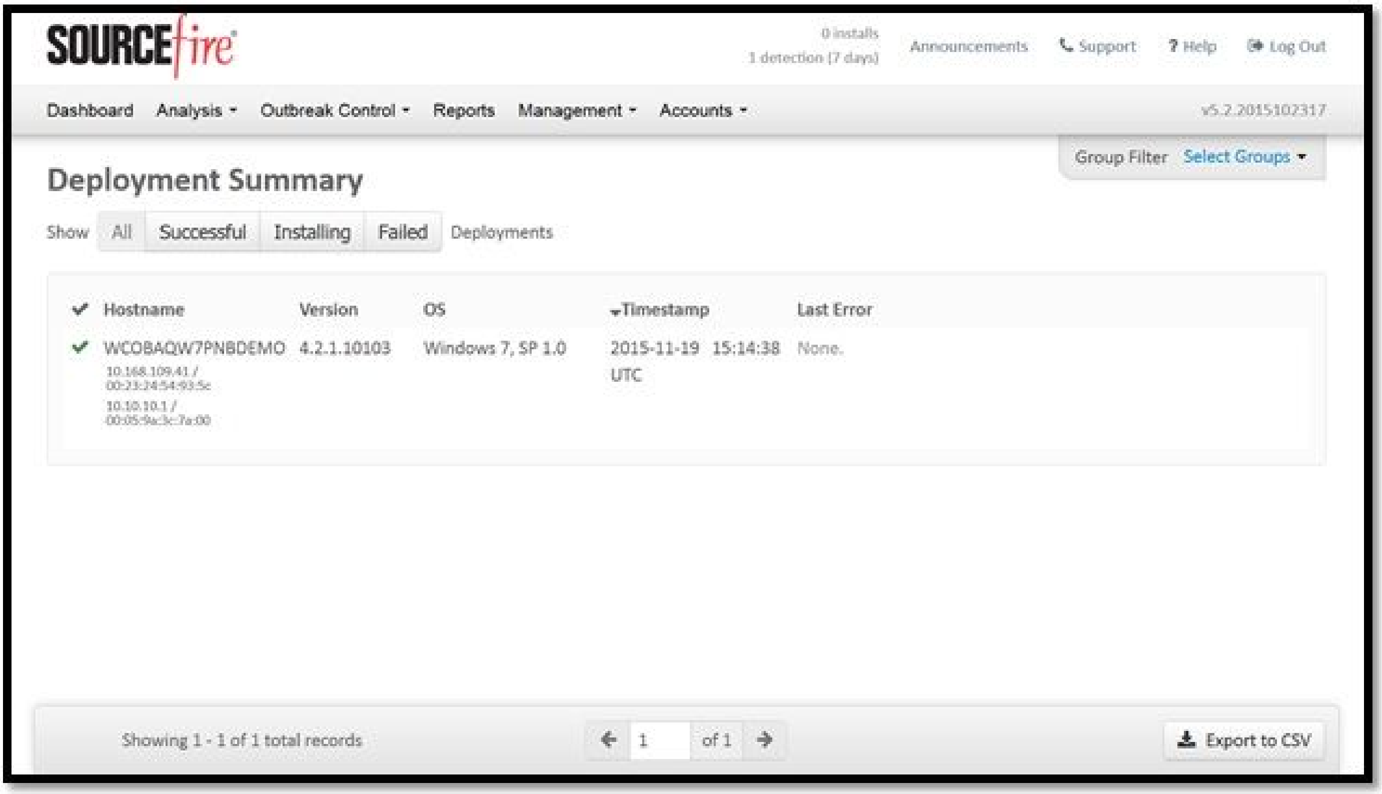
Threat Quarantined

4XpJCE_X.pdf.part has been detected as W32.Zombies.NotAVirus. Quarantine was successful.

Zombies.pdf contains Eicar string

Step 9: Deployment Summary

This page shows you a list of successful and failed FireAMP connector installs as well as those currently in progress. You can go to **Management > Deployment Summary**.



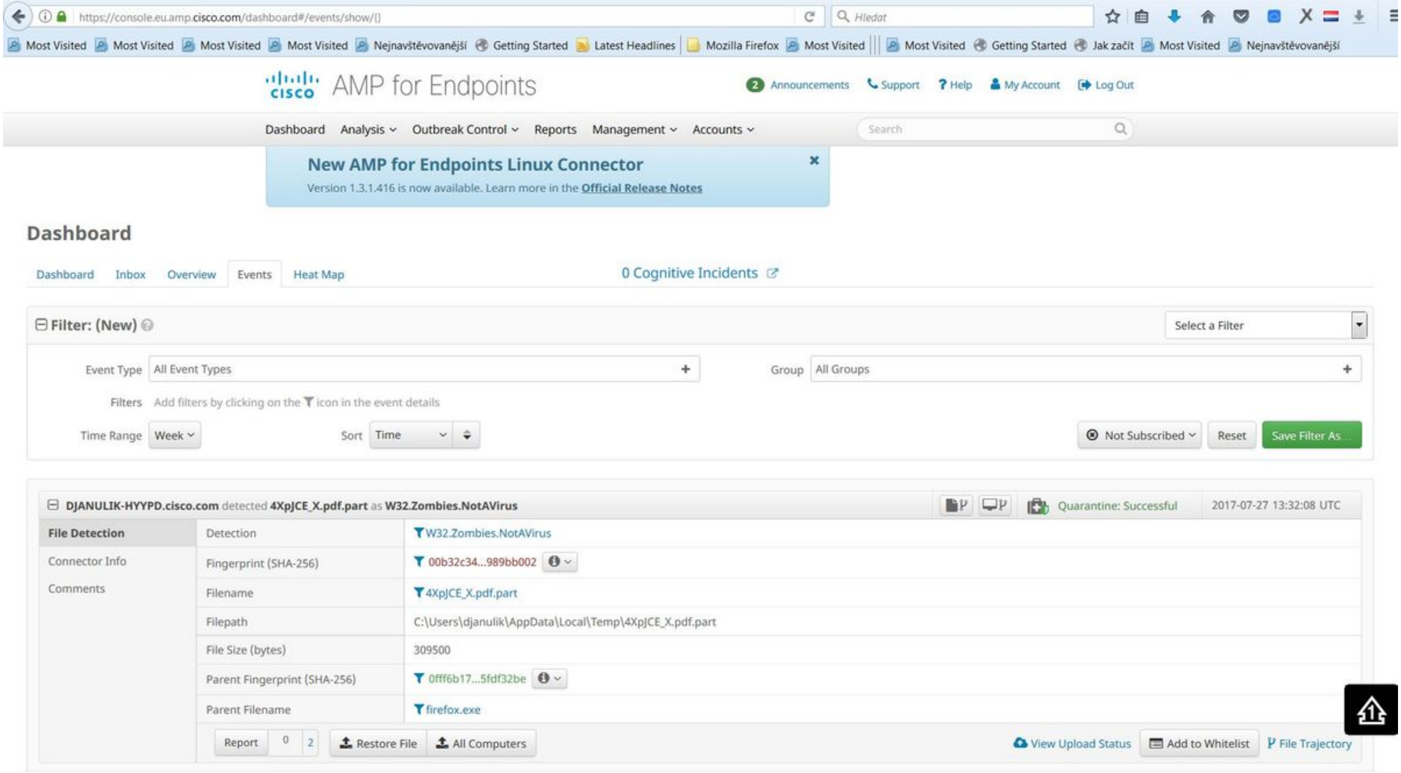
Deployment Summary

✓	Hostname	Version	OS	Timestamp	Last Error
✓	WCOBAQW7PNBDEMO 10.168.109.41 / 00:23:24:54:93:5c 10.10.10.1 / 00:05:9a:3c:7a:00	4.2.1.10103	Windows 7, SP 1.0	2015-11-19 15:14:38 UTC	None.

Showing 1 - 1 of 1 total records 1 of 1

Step 10: Thread Detection Verification

Zombies.pdf triggered an quarantine event, send to the AMP dashboard.



New AMP for Endpoints Linux Connector
Version 1.3.1.416 is now available. Learn more in the Official Release Notes

Dashboard

Filter: (New)

Event Type: All Event Types
Group: All Groups
Filters: Add filters by clicking on the icon in the event details
Time Range: Week
Sort: Time

DJANULIK-HYYPD.cisco.com detected 4XpJCE_X.pdf.part as W32.Zombies.NotAVirus — Quarantine: Successful — 2017-07-27 13:32:08 UTC

File Detection | Connector Info | Comments

Detection	W32.Zombies.NotAVirus
Fingerprint (SHA-256)	00b32c34...989bb002
Filename	4XpJCE_X.pdf.part
Filepath	C:\Users\djanulik\AppData\Local\Temp\4XpJCE_X.pdf.part
File Size (bytes)	309500
Parent Fingerprint (SHA-256)	0fff6b17...5fdf32be
Parent Filename	firefox.exe

Quarantine event

Additional Information

To get your AMP account, you can sign up for the ATS University. This gives you an overview of AMP functionality in LAB.

Related Information

- **Configure AMP Enabler**
- **Technical Support & Documentation - Cisco Systems**