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

Contents

Introduction

This document describes the method to install and configure the Advanced Malware Protection (AMP) module on an end-user system with AnyConnect.

The AnyConnect AMP Enabler is used as a medium to deploy AMP for Endpoints. It pushes the AMP for Endpoints software to a subset of endpoints from a server hosted locally within the enterprise and installs AMP services to its existing user base. This approach provides AnyConnect user base administrators with an additional security agent that detects potential malware threats that happen in the network, removes those threats, and protects the enterprise from compromise. It saves bandwidth and time taken to download, requires no changes on the portal side, and can be done without authentication credentials being sent to the endpoints.

Prerequisites

Requirements

- AnyConnect Secure Mobility Client Version 4.x
- FireAMP / AMP for Endpoints
- AnyConnect Plus / Apex Licenses
- 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)

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

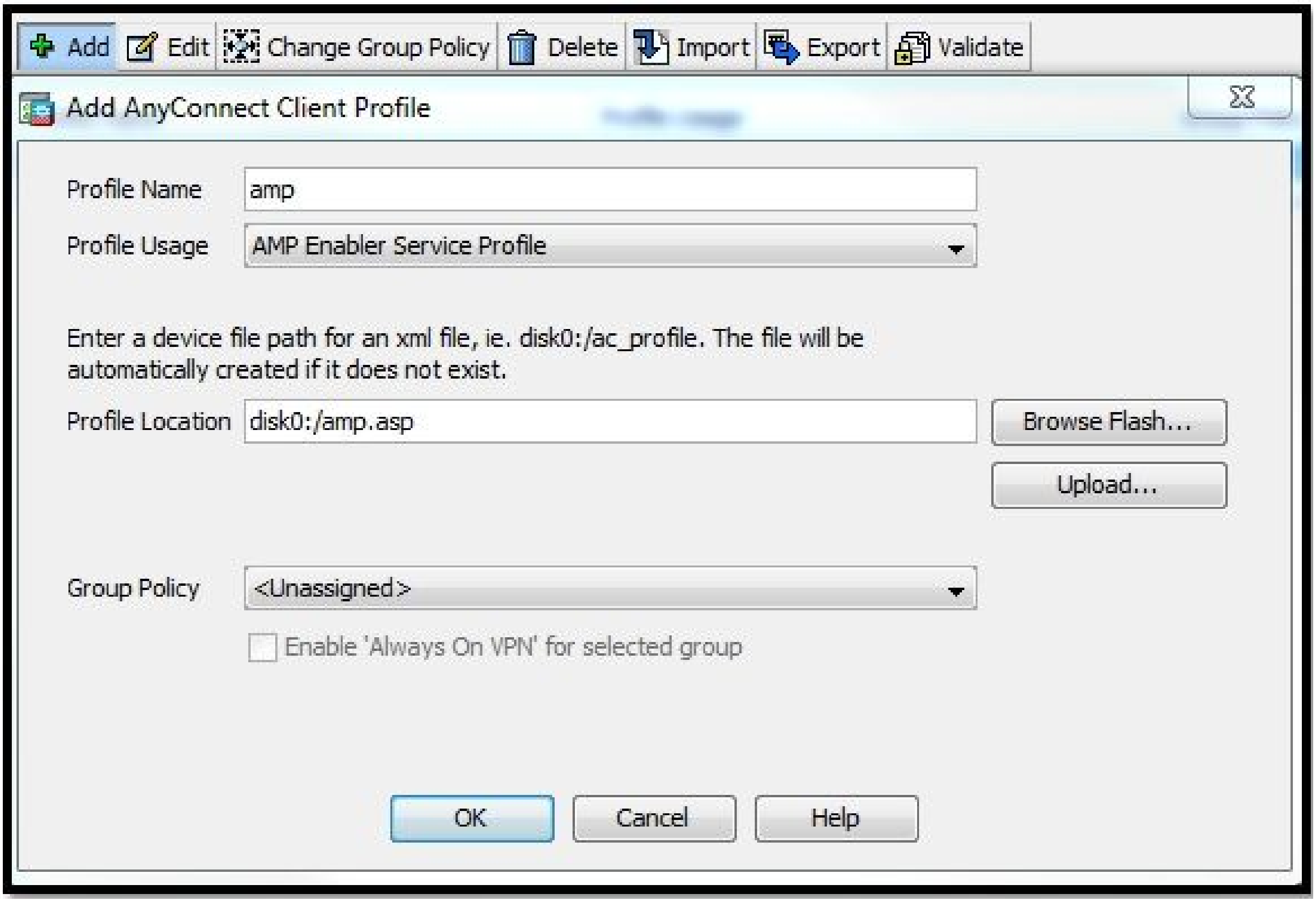
AnyConnect Deployment for AMP Enabler through ASA

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.
- Edit the AMP Profile in order to get the configuration from a web server.
- 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

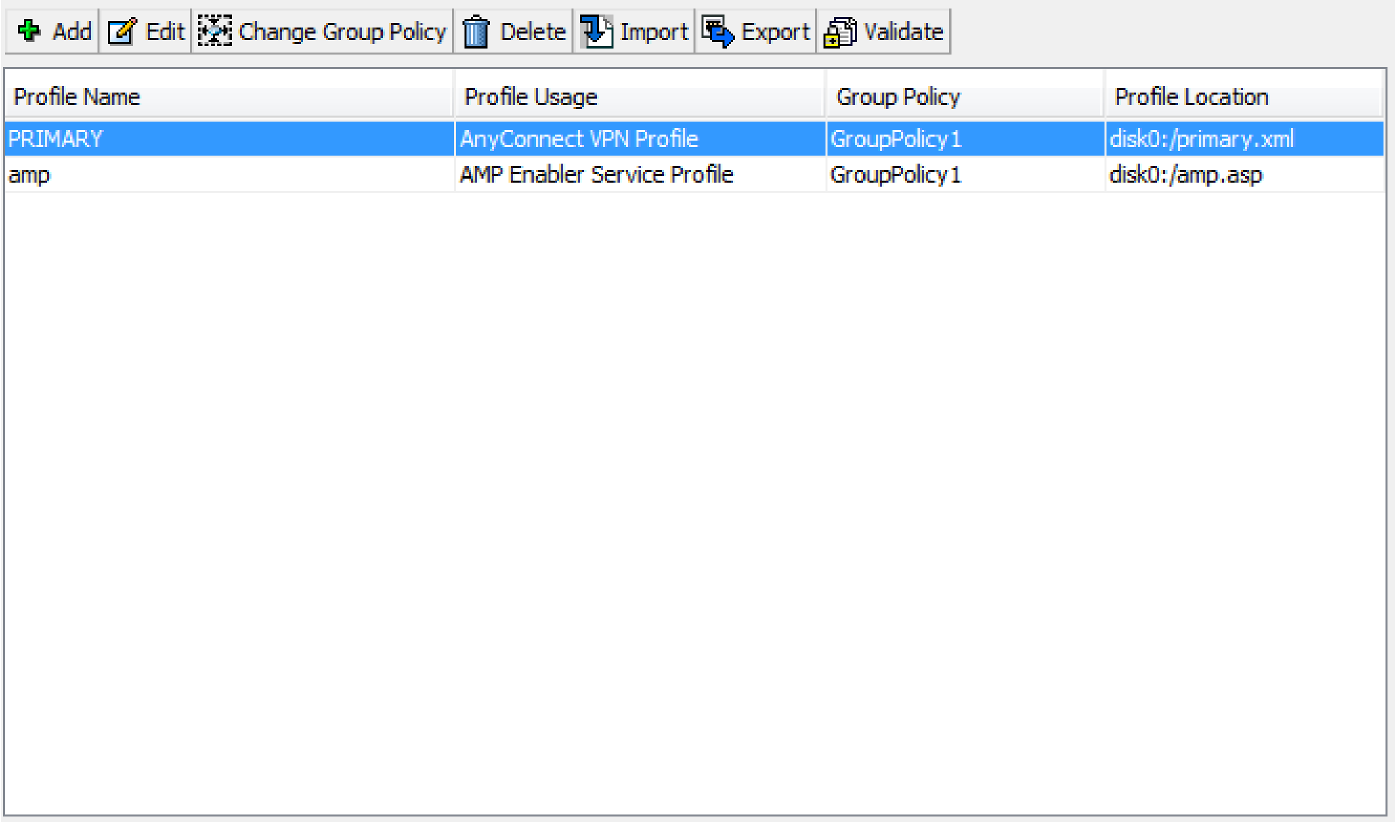
Profile Usage: AMP Enabler Service Profile

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>

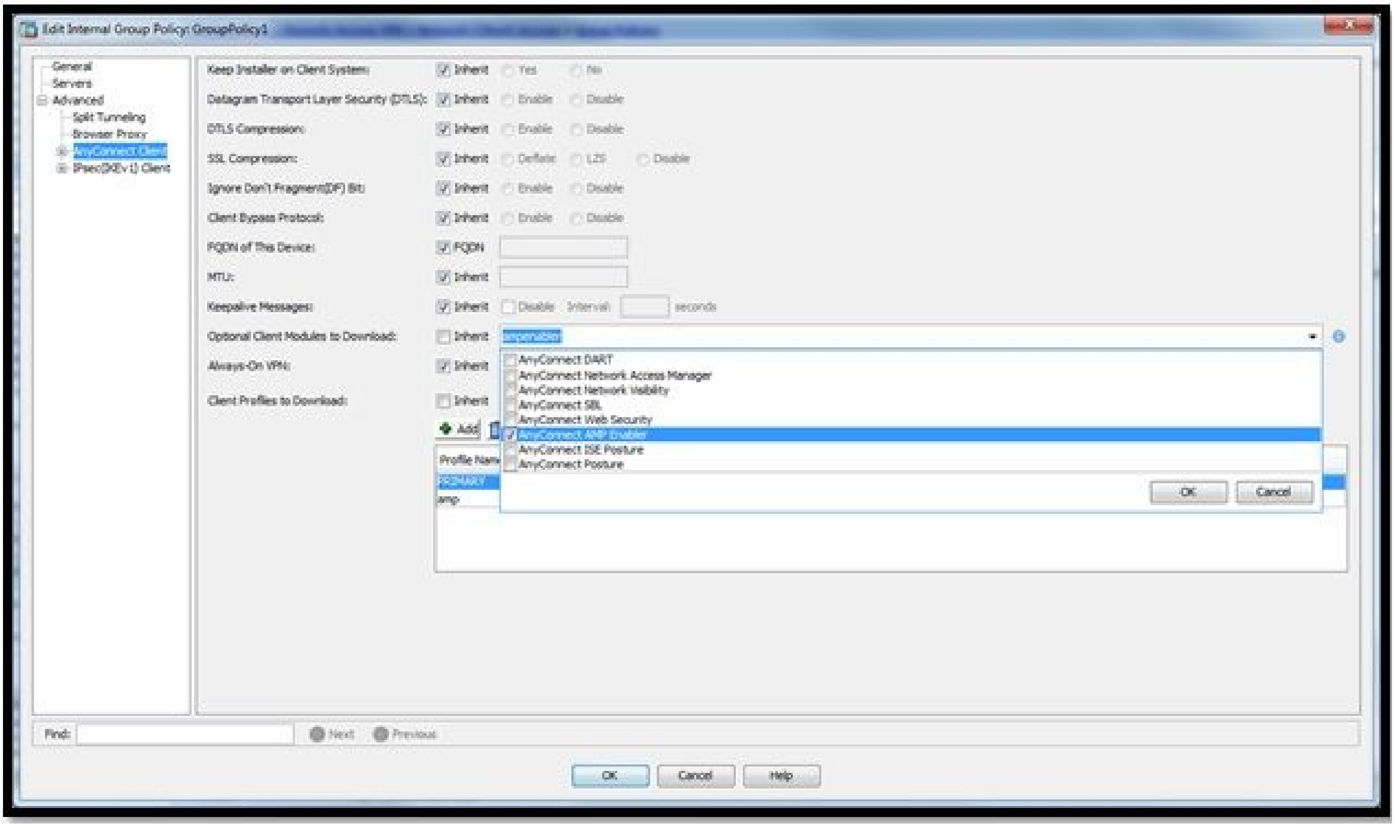
□ Enable 'Always On VPN' for selected group



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

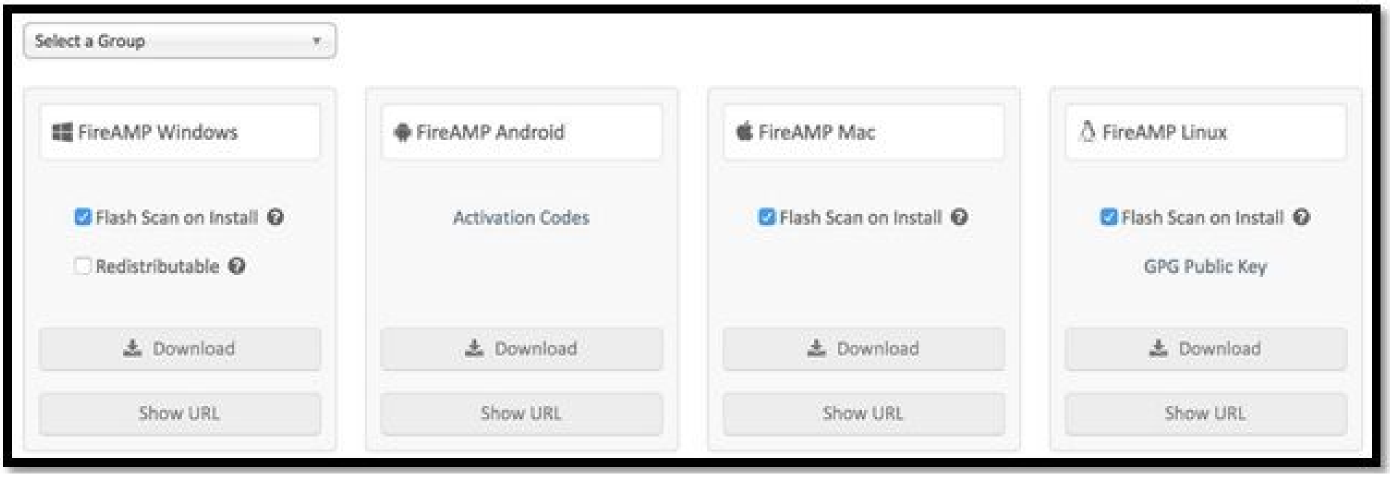
Note: Before you proceed, determine if your system meets the requirements for the AMP of Endpoints Windows Connector.

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.

Operating System	Processor	Memory	Disk Space, Cloud Only Mode	Disk Space
Microsoft Windows XP with Service Pack 3 or later	500 MHz or faster processor	256 MB RAM	150 MB available hard disk space - Cloud-only mode	1GB available hard disk space - TETRA
Microsoft Windows Vista with Service Pack 2 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 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 3.1.4 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 3.1.9 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

The Download Connector page allows you to either download the install packages for each type of FireAMP connector or copy the URL where they can be downloaded. This package can be placed on a network share or distributed via management software. The download URL can be emailed to users in order to allow them to download and install it themselves which can be downloaded for remote users.



FireAMP Windows: ☑ Flash Scan on Install, □ Redistributable

FireAMP Mac: ☑ Flash Scan on Install

FireAMP Linux: ☑ Flash Scan on Install

Select a Group

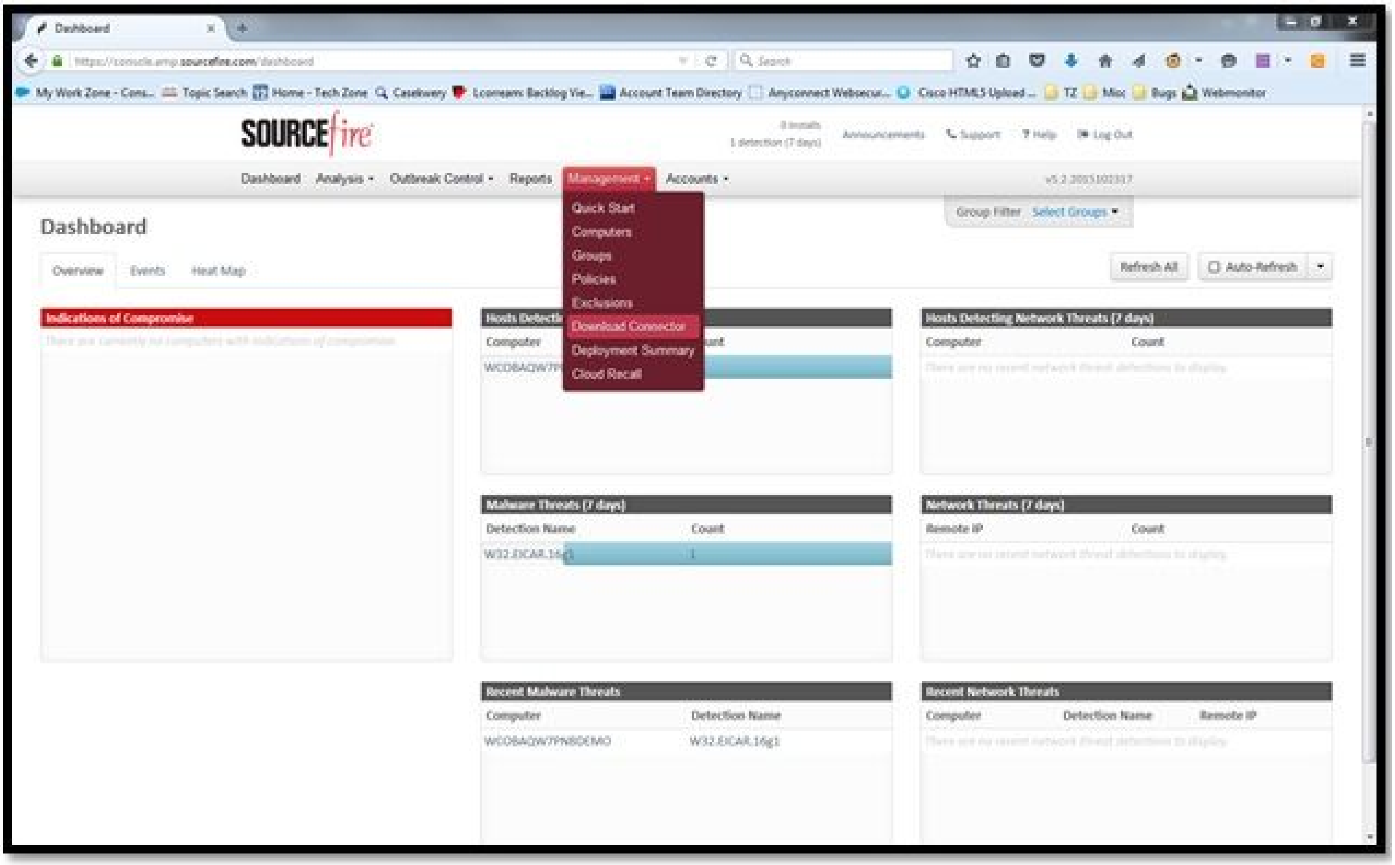
- **Audit Only:** Used when you are still learning about the product and want to install it without any impact to your existing systems.
- **Protect:** Used during normal operation and you want FireAMP to quarantine a file.
- **Triage:** Used when you have a known or suspected infected machine.
- **Server:** Used when you install a connector on a standard Windows server.
- **Domain Controller:** Used when you install a connector on a Windows Domain Controller.

Features

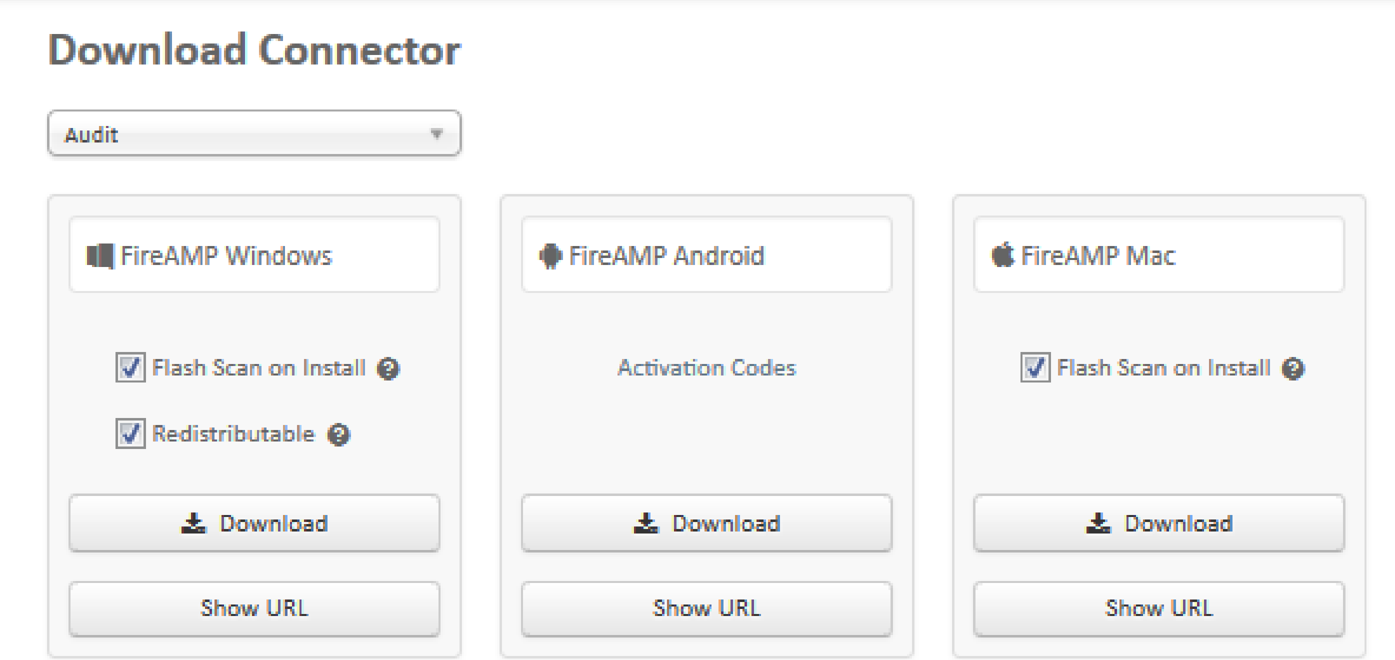
- **Flash Scan on Install:** Scan process runs during the installation. This scan is cloud-based and requires a network connection. It is relatively quick to perform.
- **Redistributable:** This option downloads 32-bit and 64-bit installers in one single package.

> **Note**: By default, it downloads a small (~500 KB) bootstrapper file to install the FireAMP Connector. This executable determines if the computer runs a 32 or 64-bit operating system and downloads and installs the appropriate version of the FireAMP Connector.
>
> However, for VPN purposes, you should choose to download a redistributable installer. This is a 30 MB file that contains both the 32 and 64-bit installers. This file can be placed on a network share or pushed to all the computers in a group via a tool like System Center Configuration Manager in order to install the FireAMP Connector on multiple computers. The bootstrapper and redistributable installer also both contain a `policy.xml` file that is used as a configuration file for the install.

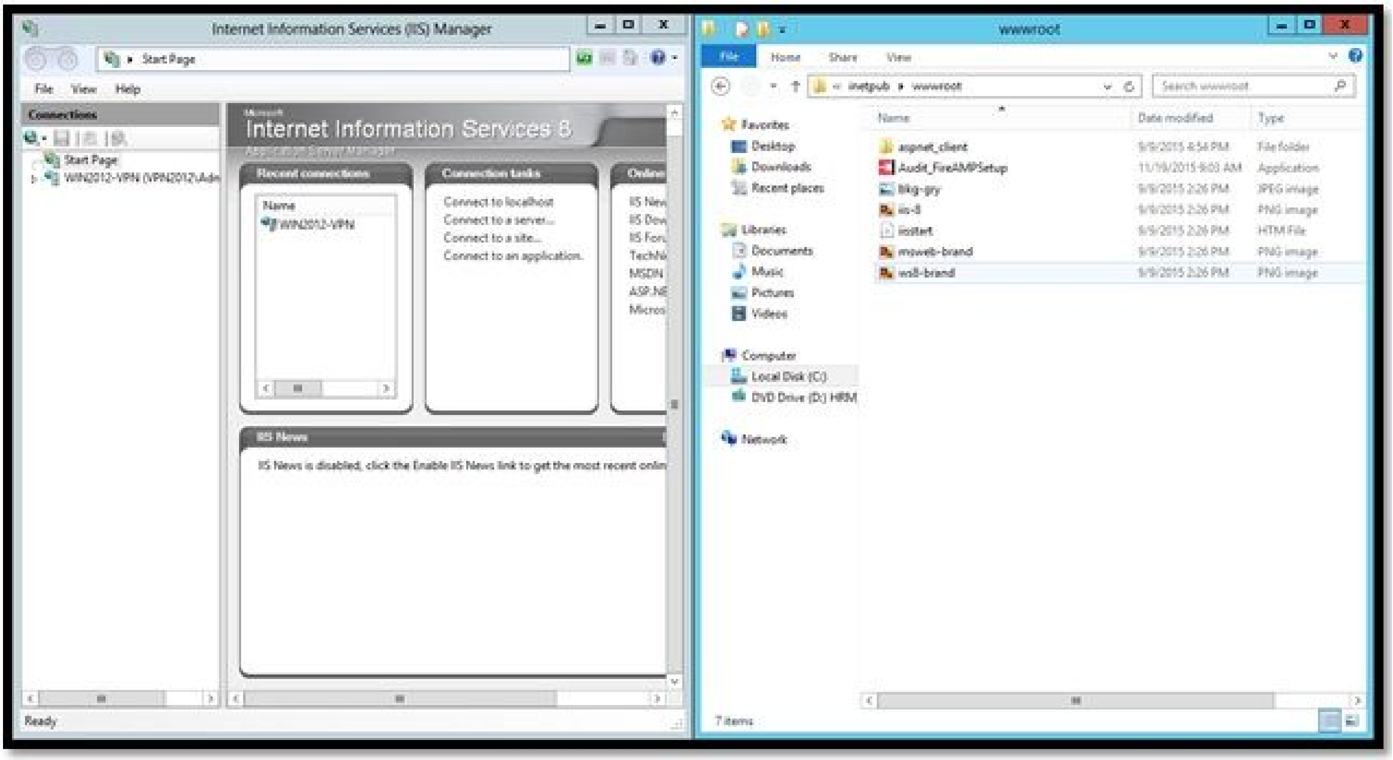
In order to download the connector, navigate to **Management > Download Connector**. Then choose type, and **Download** FireAMP (Windows, Android, Mac, Linux).



In this case, the **Audit** option for the **Download Connector** and the installation for Windows Machine was chosen.



Note: When this file is downloaded it generates an `.exe` file called, in this case, `Audit_FireAMPSetup.exe`. This file was sent to the web server in order to be available and downloaded from the ASA once the user asks for the configuration for AMP.



IIS News is disabled, click the Enable IIS News link to get the most recent onlin

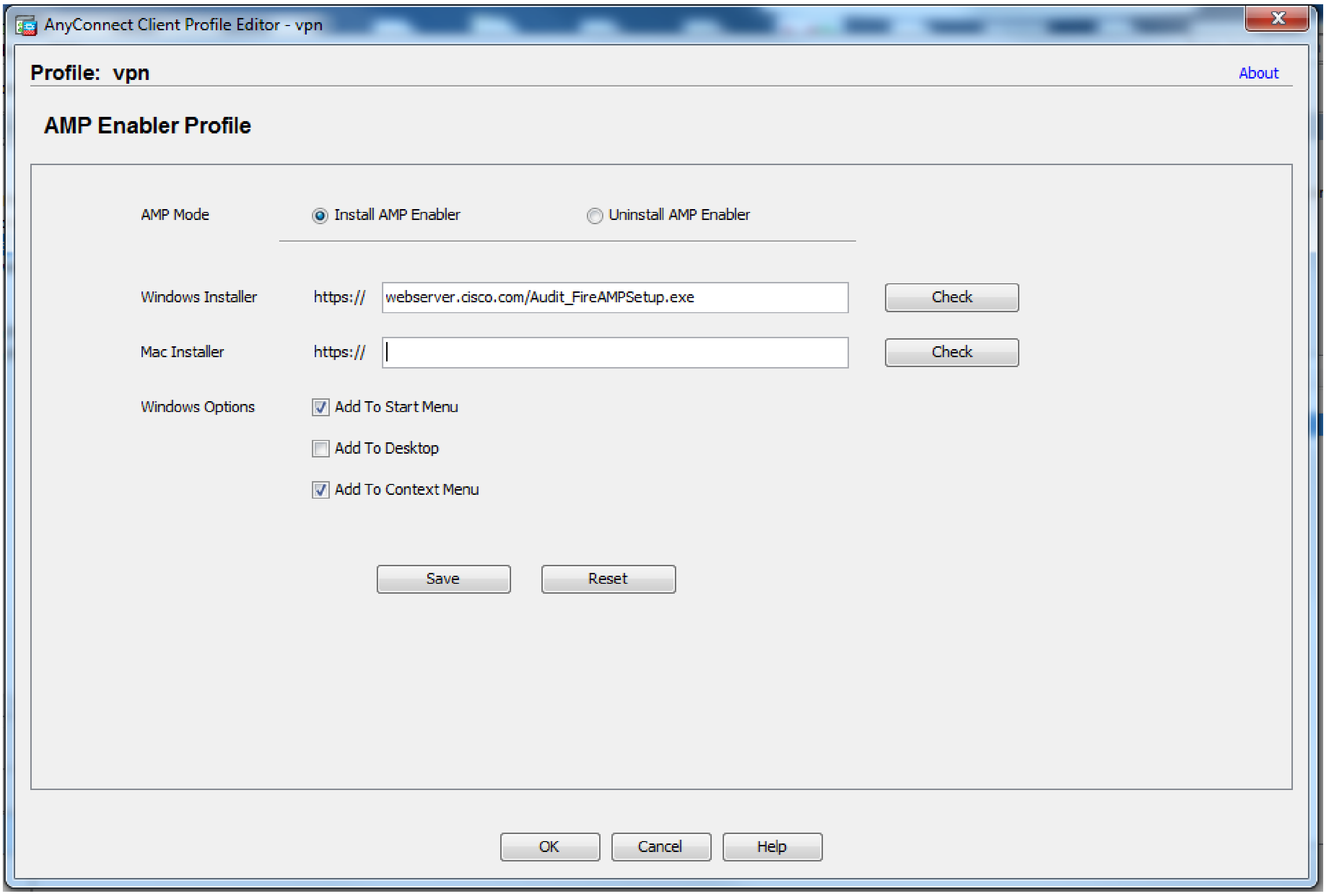
Name	Date modified	Type
aspnet_client	9/9/2015 4:54 PM	File folder
Audit_FireAMPSetup	11/19/2015 9:03 AM	Application
bkg-gry	9/9/2015 2:26 PM	JPEG image
iis-8	9/9/2015 2:26 PM	PNG image
iisstart	9/9/2015 2:26 PM	HTM File
msweb-brand	9/9/2015 2:26 PM	PNG image
ws8-brand	9/9/2015 2:26 PM	PNG image

Step 4: Download the Web Security Client Profile

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.



AnyConnect Client Profile Editor - vpn

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

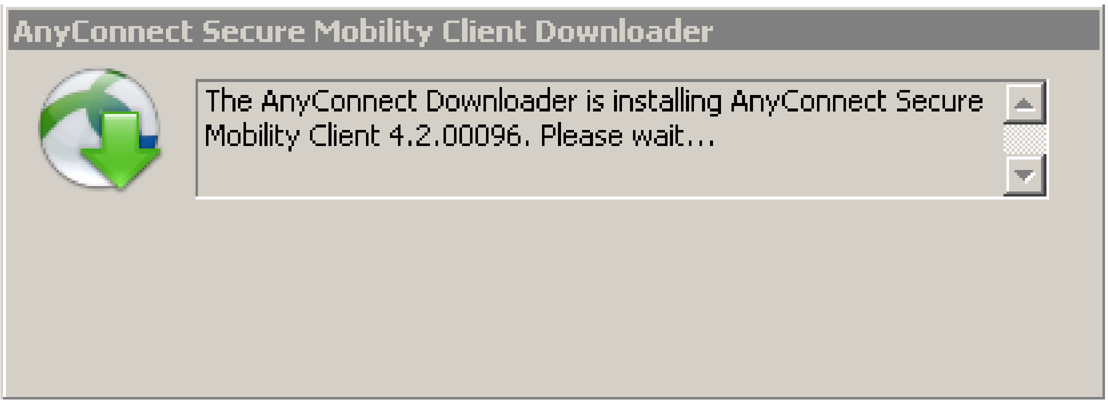
☑ Add To Start Menu

□ 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.

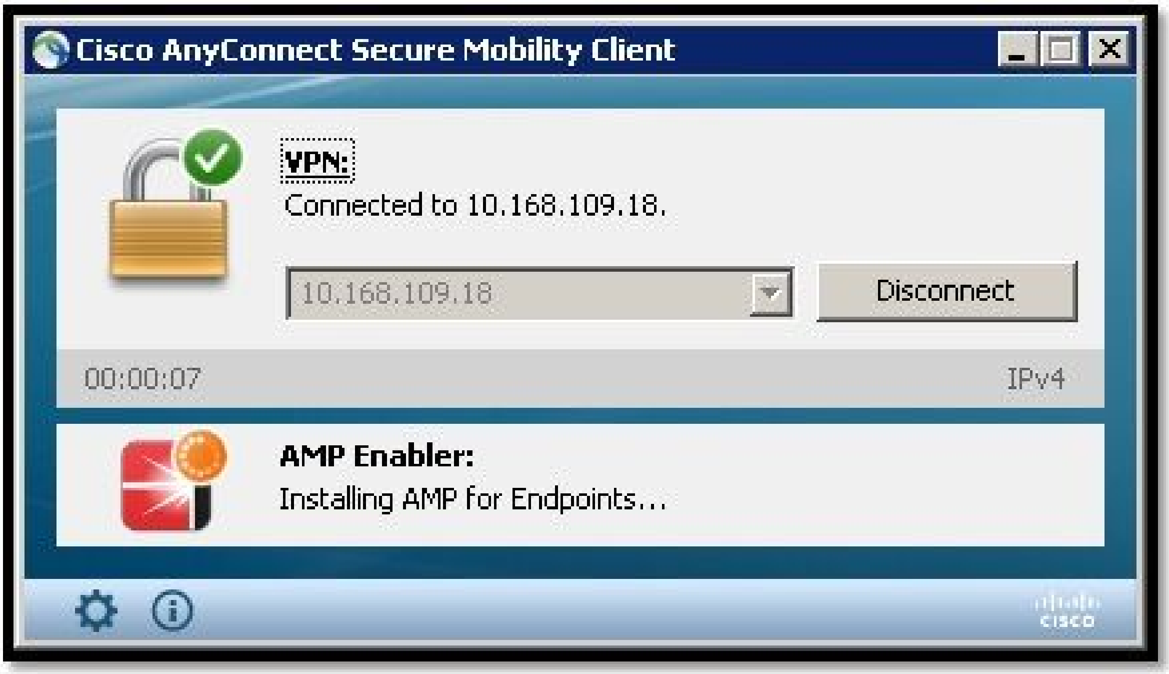


AnyConnect Secure Mobility Client Downloader

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

Step 6: Verify the VPN Connection and the AMP Enabler

Verify if the VPN is connected and the **AMP Enabler** collects configuration from the web server.



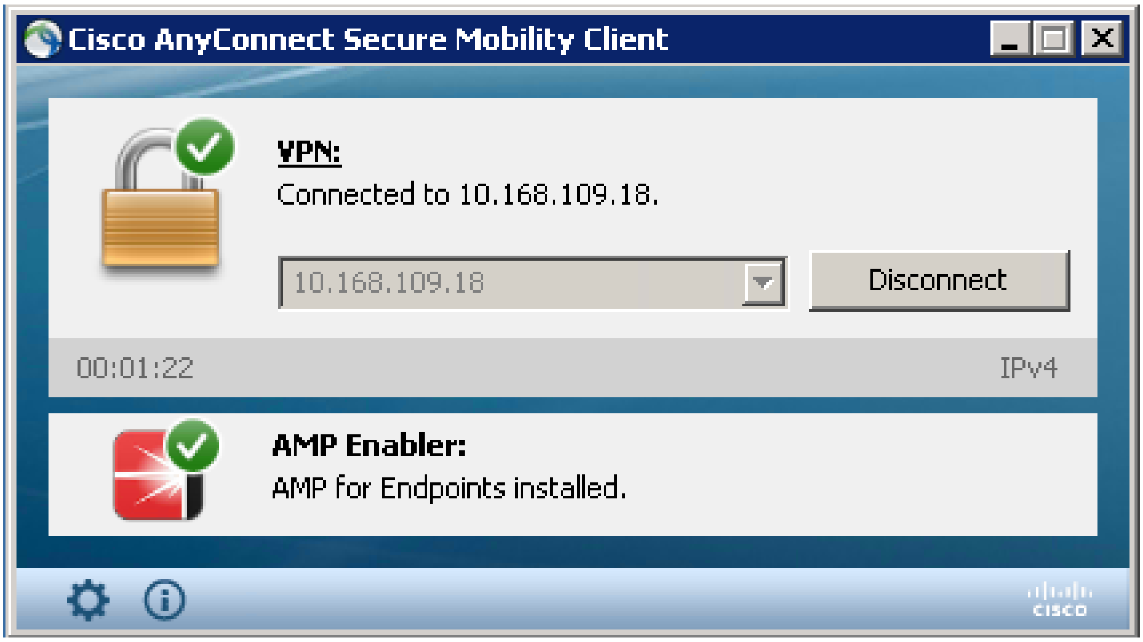
Cisco AnyConnect Secure Mobility Client

VPN:
Connected to 10.168.109.18.

AMP Enabler:
Installing AMP for Endpoints...

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.



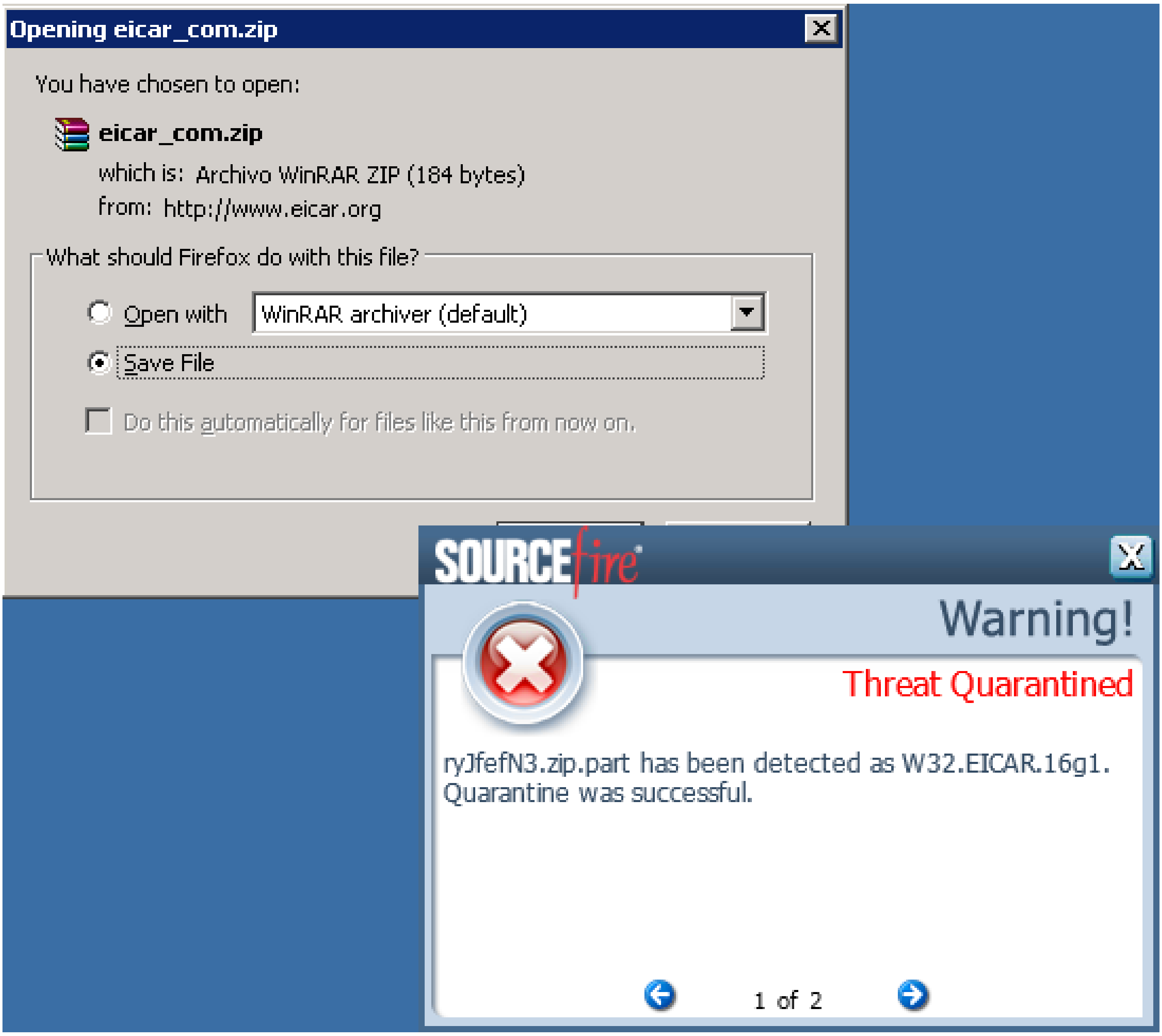
Cisco AnyConnect Secure Mobility Client

VPN:
Connected to 10.168.109.18.

AMP Enabler:
AMP for Endpoints installed.

Step 8: Test with an Eicar String Contained in a Zip File in a Computer

Test with an Eicar string contained in a zip file in a computer in order to verify if everything works as expected.



Opening eicar_com.zip

You have chosen to open:

eicar_com.zip

which is: Archivo WinRAR ZIP (184 bytes)

from: http://www.eicar.org

What should Firefox do with this file?

○ Open with WinRAR archiver (default)

● Save File

□ Do this automatically for files like this from now on.

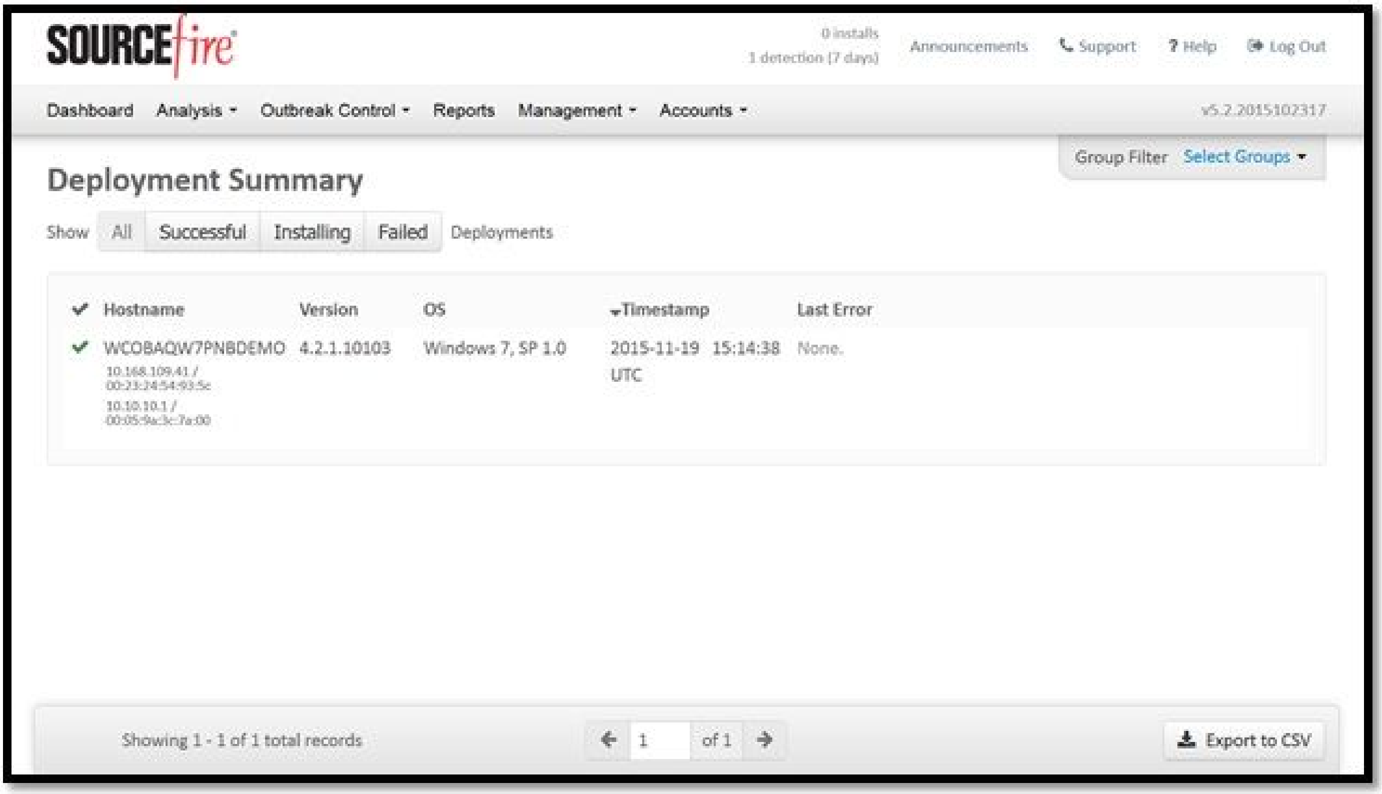
Warning!

Threat Quarantined

ryJfefN3.zip.part has been detected as W32.EICAR.16g1. Quarantine was successful.

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

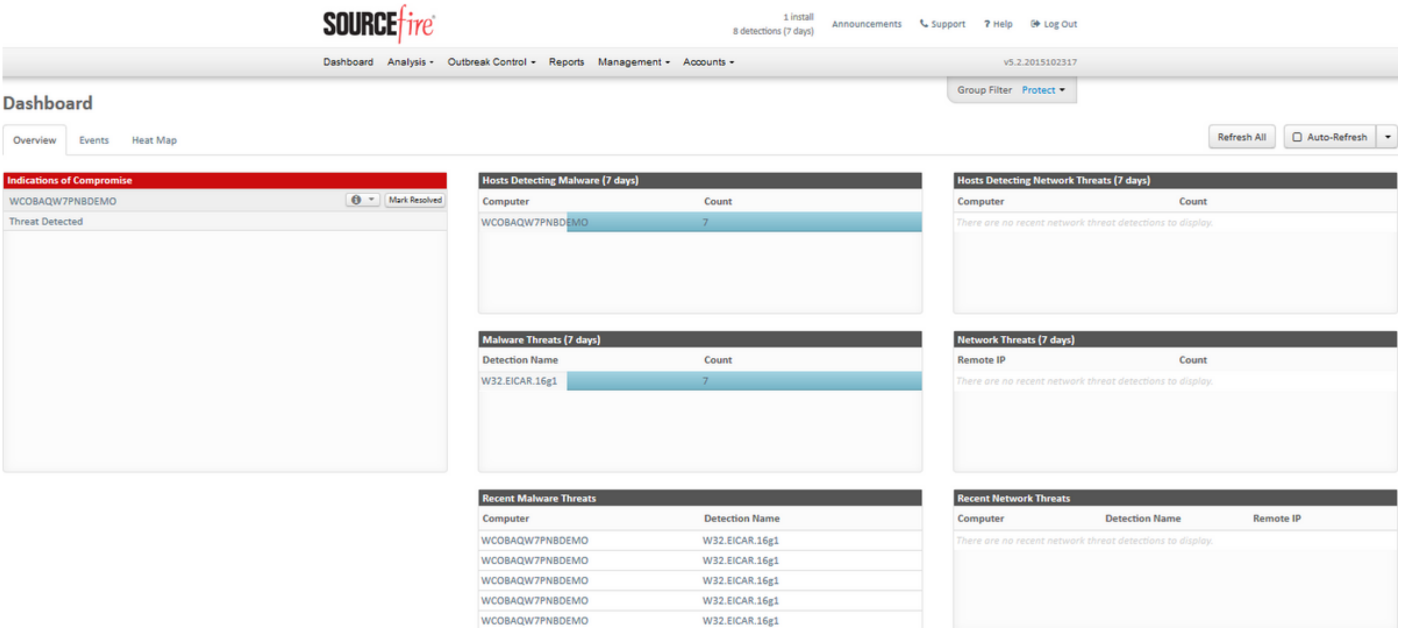
✓	Hostname	Version	OS	Timestamp	Last Error
✓	WCOBAQW7PNBDEMO 10.168.109.41 / 00:23:24:54:93:5c 10.10.10.1 / 00:05:9a:3c:7a:00	4.2.1.10103	Windows 7, SP 1.0	2015-11-19 15:14:38 UTC	None.

Showing 1 - 1 of 1 total records

1 of 1

Step 10: Thread Detection Verification

This page shows you a list of threads blocked by the FireAMP connector and also the machines impacted. You can go to the **Dashboard**.



Dashboard

Indications of Compromise

WCOBAQW7PNBDEMO

Threat Detected

Hosts Detecting Malware (7 days)

Computer	Count
WCOBAQW7PNBDEMO	7

Malware Threats (7 days)

Detection Name	Count
W32.EICAR.16g1	7

Recent Malware Threats

Computer	Detection Name
WCOBAQW7PNBDEMO	W32.EICAR.16g1
WCOBAQW7PNBDEMO	W32.EICAR.16g1
WCOBAQW7PNBDEMO	W32.EICAR.16g1
WCOBAQW7PNBDEMO	W32.EICAR.16g1
WCOBAQW7PNBDEMO	W32.EICAR.16g1

Hosts Detecting Network Threats (7 days)

Computer	Count

There are no recent network threat detections to display.

Network Threats (7 days)

Remote IP	Count

There are no recent network threat detections to display.

Recent Network Threats

Computer	Detection Name	Remote IP

There are no recent network threat detections to display.

Additional Information

Incompatible Software for FireAMP Windows Connector are:

- Zone Alarm by Check Point
- Carbon Black
- Res Software AppGuard

Related Information

- [Configure AMP Enabler]
- [Technical Support & Documentation - Cisco Systems]