AnyConnect 4.x 및 AMP Enabler를 통한 AMP 모듈의 설치 및 컨피그레이션

목차

소개

이 문서에서는 AnyConnect를 사용하여 최종 사용자 시스템에서 AMP(Advanced Malware Protection) 모듈을 설치하고 구성하는 방법을 설명합니다.

AnyConnect AMP Enabler는 엔드포인트용 AMP를 구축하기 위한 매체로 사용됩니다. AMP Enabler는 엔터프라이즈 내의 로컬로 호스팅되는 서버에서 엔드포인트 하위 집합으로 엔드포인트용 AMP 소프트웨어를 푸시하고 기존 사용자 기반에 대해 AMP 서비스를 설치합니다. 이러한 접근 방식을 통해 AnyConnect 사용자 기반 관리자에게는 네트워크에서 발생할 수 있는 악성코드 위협을 탐지하고 제거하며 엔터프라이즈의 데이터 손상을 보호하는 추가 보안 에이전트가 제공됩니다. AMP Enabler가 있으면 대역폭과 다운로드에 소요되는 시간이 줄어들고, 포털 측 변경도 하지 않아도 되며, 엔드포인트로 인증 크리덴셜을 보내지 않고도 필요한 작업을 수행할 수 있습니다.

사전 요구 사항

요구 사항

- AnyConnect Secure Mobility Client 버전 4.x

- FireAMP/AMP for Endpoints
- AnyConnect Plus/Apex 라이선스
- ASDM 버전 7.3.2 이상

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- 소프트웨어 버전 9.5.1을 사용하는 ASA(Adaptive Security Appliance) 5525
- Microsoft Windows 7 Professional 64비트의 AnyConnect Secure Mobility Client 4.2.00096
- ASDM 버전 7.5.1(112)

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

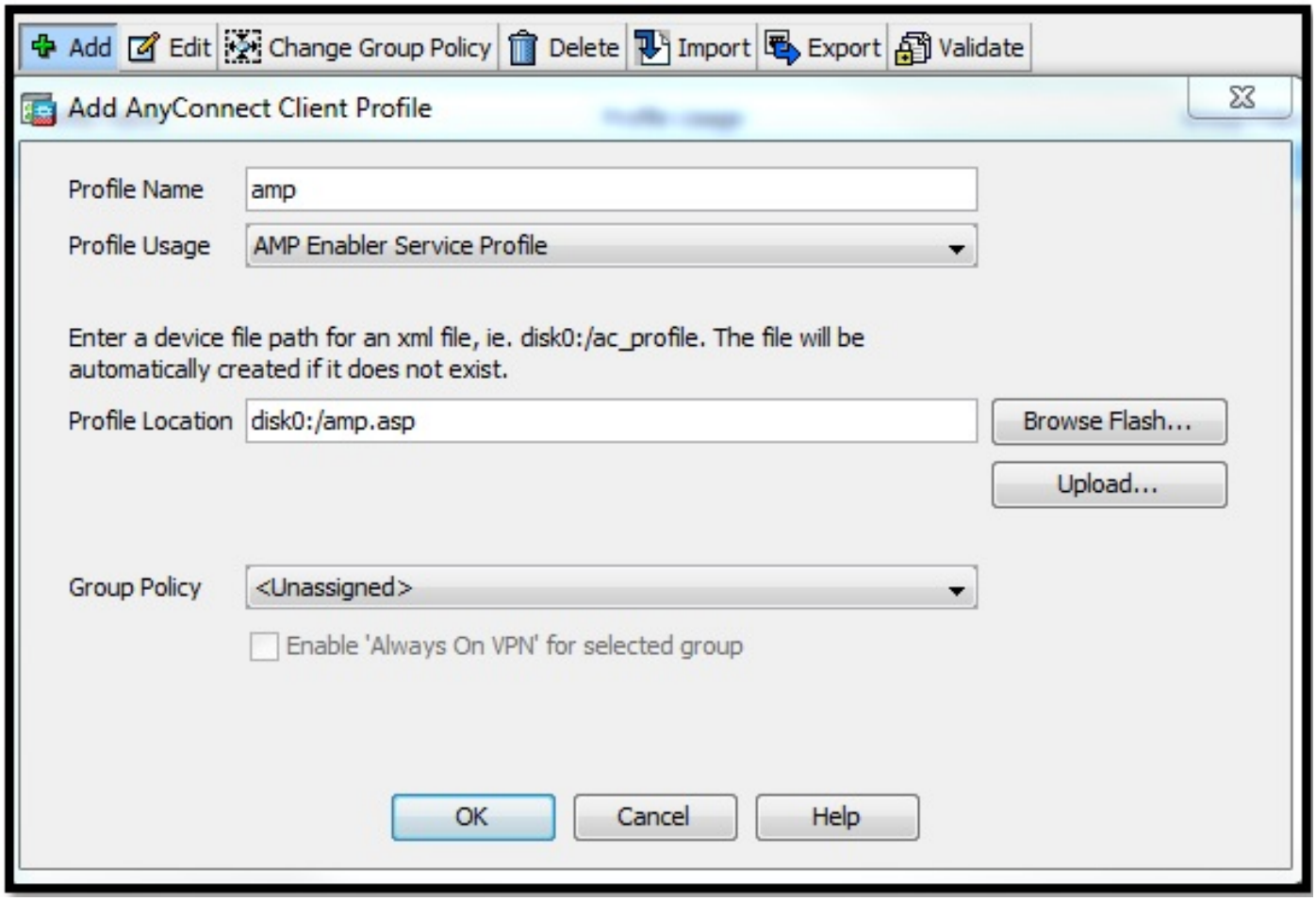
ASA를 통해 AMP Enabler용 AnyConnect 구축

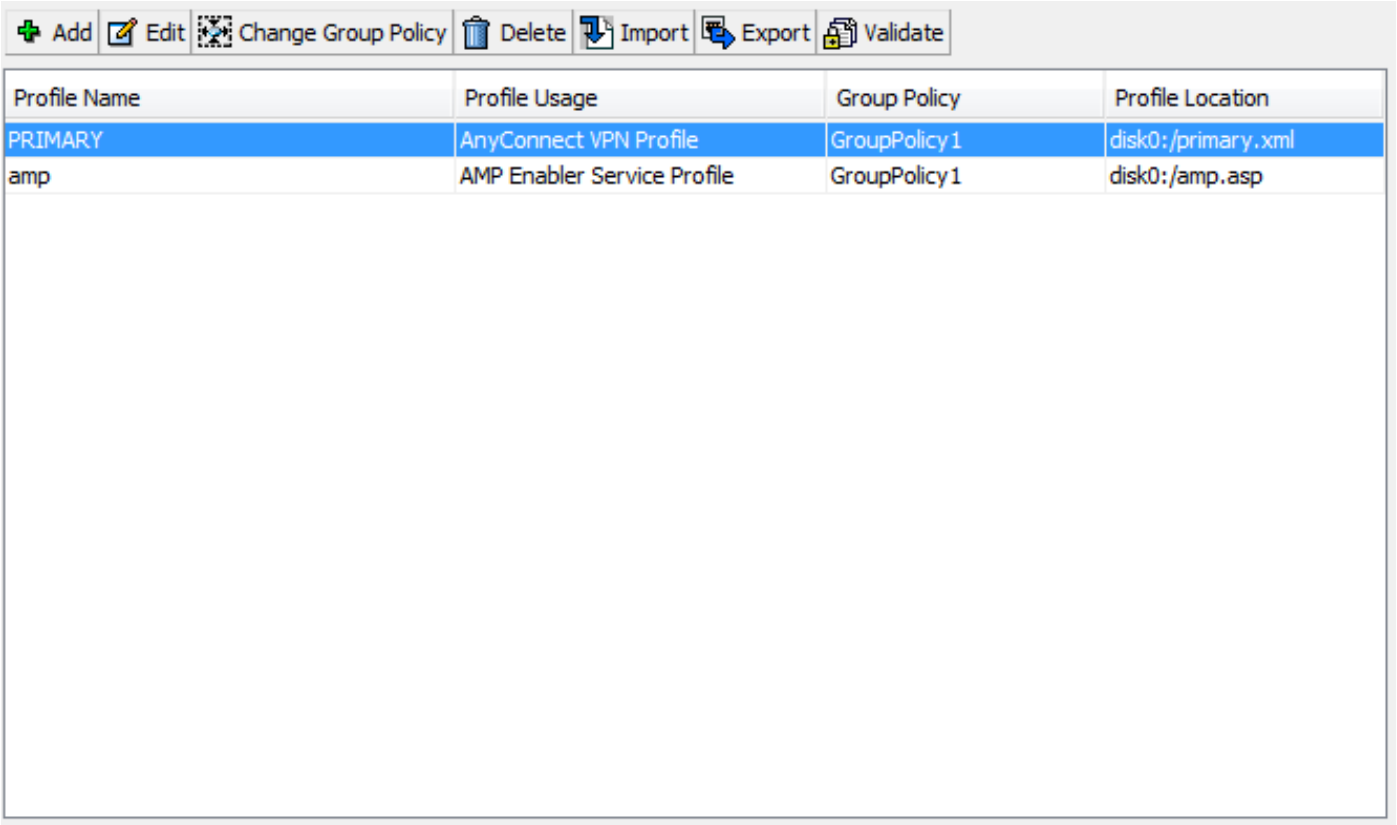
컨피그레이션에 필요한 단계는 다음과 같습니다.

- AnyConnect AMP Enabler 클라이언트 프로파일 구성
- AnyConnect VPN 그룹 정책 수정 및 AMP Enabler 서비스 프로파일 다운로드
- AMP 프로파일을 수정하여 웹 서버에서 컨피그레이션 가져오기
- 사용자 머신에서 설치 확인

1단계: AnyConnect AMP Enabler 클라이언트 프로파일 구성

- **Configuration(컨피그레이션) > Remote Access VPN(원격 액세스 VPN) > Network (Client) Access(네트워크(클라이언트) 액세스) > AnyConnect Client Profiles(AnyConnect 클라이언트 프로파일)**로 이동합니다.
- **AMP Enabler Service Profile(AMP Enabler 서비스 프로파일)**을 추가합니다.

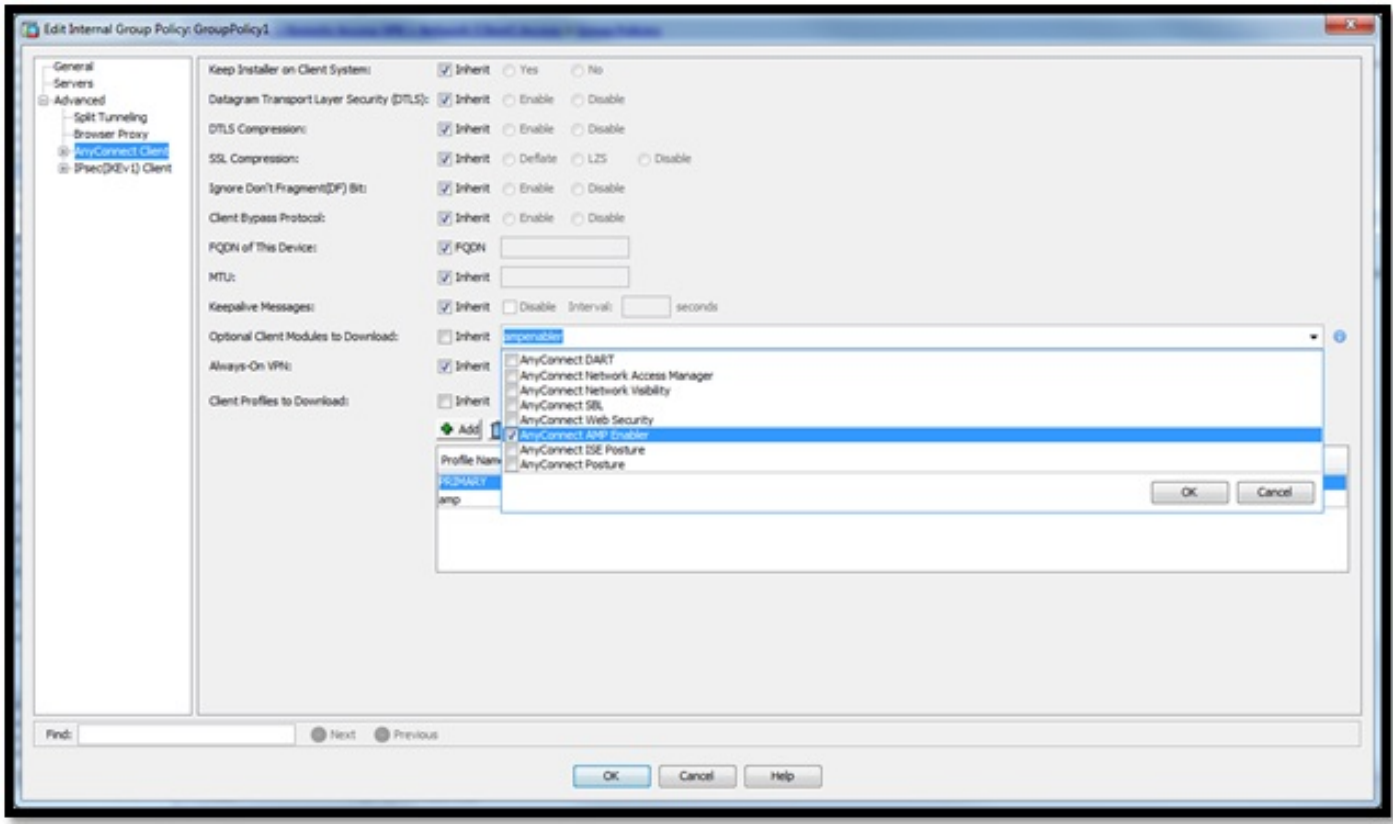




2단계: 그룹 정책을 수정하여 AnyConnect AMP Enabler 다운로드

- **Configuration(컨피그레이션) > Remote Access VPN(원격 액세스 VPN) > Group Policies(그룹 정책) > Edit(수정)**으로 이동합니다.

- **AMP Enabler Service Profile(AMP Enabler 서비스 프로파일)**을 추가합니다.



3단계: FireAMP 정책 다운로드

> **참고**: 계속 진행하기 전에 시스템이 AMP for Endpoints Windows Connector에 대한 요구 사항을 충족하는지 확인하십시오.

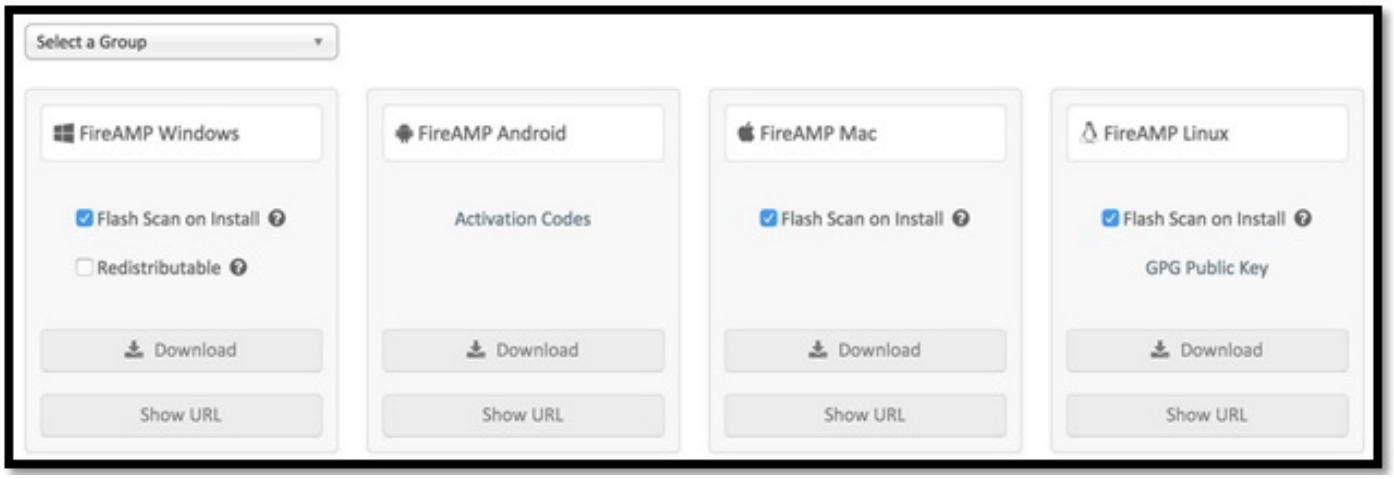
AMP for Endpoints Windows Connector의 시스템 요구 사항

Windows 운영 체제를 기반으로 한 FireAMP Connector의 최소 시스템 요구 사항은 다음과 같습니다. FireAMP Connector는 이러한 운영 체제의 32비트 및 64비트 버전을 모두 지원합니다.

Operating System(운영 체제)	프로세서	메모리	디스크 공간, 클라우드 전용 모드	디스크 공간
Microsoft Windows XP 서비스 팩 3 이상	500MHz 이상 프로세서	256MB RAM	150MB의 사용 가능한 하드 디스크 공간 - 클라우드 전용 모드	1GB의 사용 가능한 하드 디스크 공간 - TETRA
Microsoft Windows Vista 서비스 팩 2 이상	1GHz 이상 프로세서	512MB RAM	150MB의 사용 가능한 하드 디스크 공간 - 클라우드 전용 모드	1GB의 사용 가능한 하드 디스크 공간 - TETRA
Microsoft Windows 7	1GHz 이상 프로세서	1 GB RAM	150MB의 사용 가능한 하드 디스크 공간 - 클라우드 전용 모드	1GB의 사용 가능한 하드 디스크 공간 - TETRA
Microsoft Windows 8 및 8.1(FireAMP	1GHz 이상 프로세서	512MB RAM	150MB의 사용 가능한 하드 디스크 공간 - 클라우드	1GB의 사용 가능한 하드 디스크 공간 - TETRA

Connector 3.1.4 이상 필요)			전용 모드	
Microsoft Windows Server 2003	1GHz 이상 프로세서	512MB RAM	150MB의 사용 가능한 하드 디스크 공간 - 클라우드 전용 모드	1GB의 사용 가능한 하드 디스크 공간 - TETRA
Microsoft Windows Server 2008	2GHz 이상 프로세서	2 GB RAM	150MB의 사용 가능한 하드 디스크 공간 - 클라우드 전용 모드	1GB의 사용 가능한 하드 디스크 공간 - TETRA
Microsoft Windows Server 2012(FireAMP Connector 3.1.9 이상 필요)	2GHz 이상 프로세서	2 GB RAM	150MB의 사용 가능한 하드 디스크 공간 - 클라우드 전용 모드	1GB의 사용 가능한 하드 디스크 공간 - TETRA

Download Connector(Connector 다운로드) 페이지에서는 각 FireAMP Connector 유형의 설치 패키지를 다운로드하거나 이러한 패키지를 다운로드할 수 있는 URL을 복사할 수 있습니다. 이러한 패키지는 네트워크 공유에 저장하거나 관리 소프트웨어를 통해 배포할 수 있습니다. 다운로드 URL을 이메일로 사용자에게 보내면 사용자가 설치 패키지를 직접 다운로드하여 설치할 수 있으므로 원격 사용자가 다운로드할 수 있습니다.



그룹 선택

- **Audit Only(감사 전용):** 제품에 대해 계속 알아보는 중이며 기존 시스템에 영향을 주지 않는 상태로 제품을 설치하려는 경우에 사용됩니다.
- **Protect(보호):** 정상적인 작동 중에 FireAMP에서 파일을 격리하려는 경우에 사용됩니다.
- **Triage(분류):** 알려져 있거나 의심되는 감염 머신이 있는 경우에 사용됩니다.
- **Server(서버):** 표준 Windows 서버에 커넥터를 설치할 때 사용됩니다.
- **Domain Controller(도메인 컨트롤러):** Windows 도메인 컨트롤러에 커넥터를 설치할 때 사용됩니다.

기능

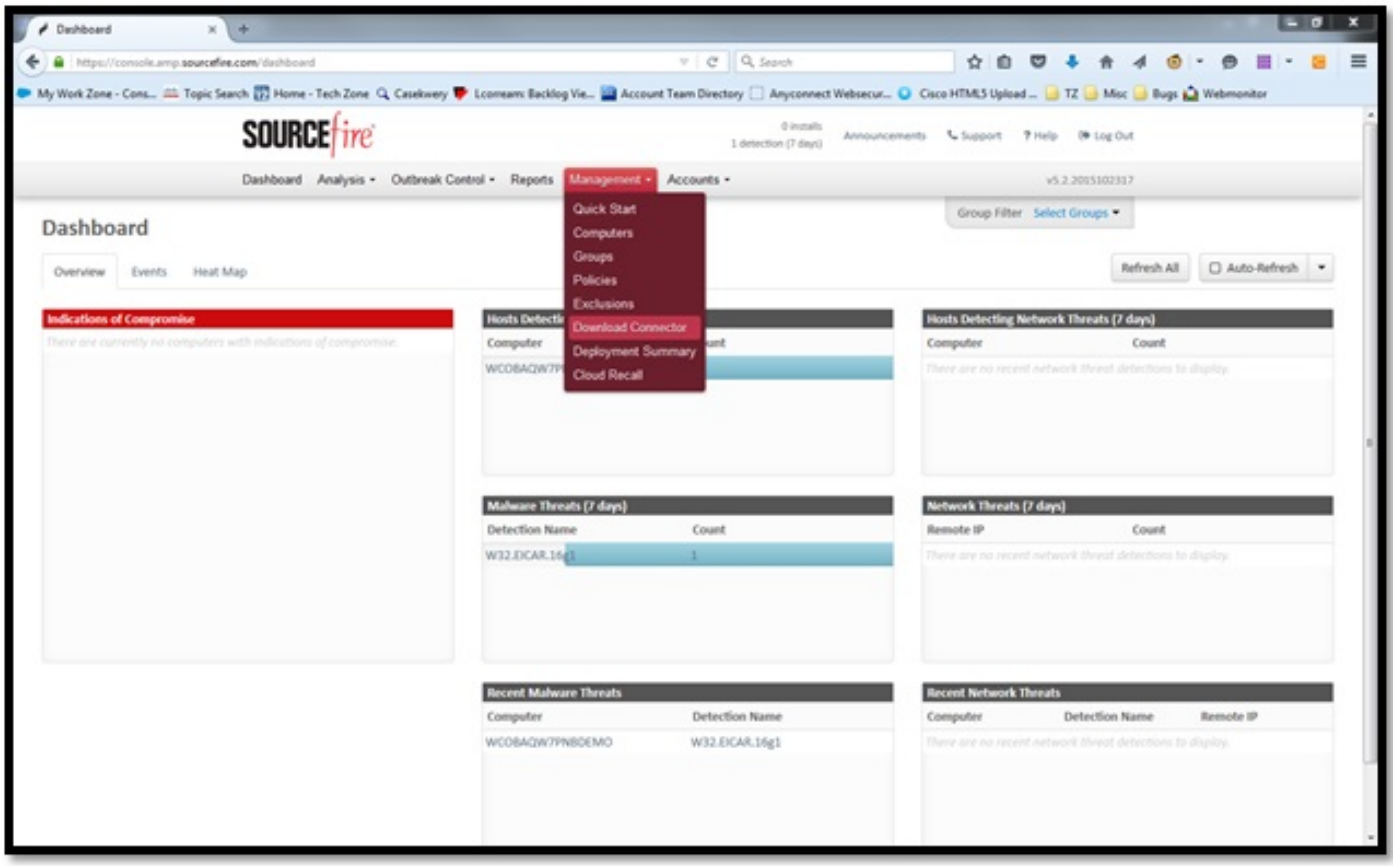
- **Flash Scan on Install(설치 시 Flash 스캔):** 설치하는 동안 스캔 프로세스가 실행됩니다. 이 스캔은 클라우드를 기반으로 하며 네트워크 연결이 필요하고, 상대적으로 빠르게 수행됩니다.
- **Redistributable(재배포 가능):** 이 옵션은 단일 패키지로 된 32비트 및 64비트 설치 프로그램을 다운로드합니다.

참고: 기본적으로 FireAMP Connector 설치를 위해 500KB 이하의 작은 부트스트래퍼 파일을

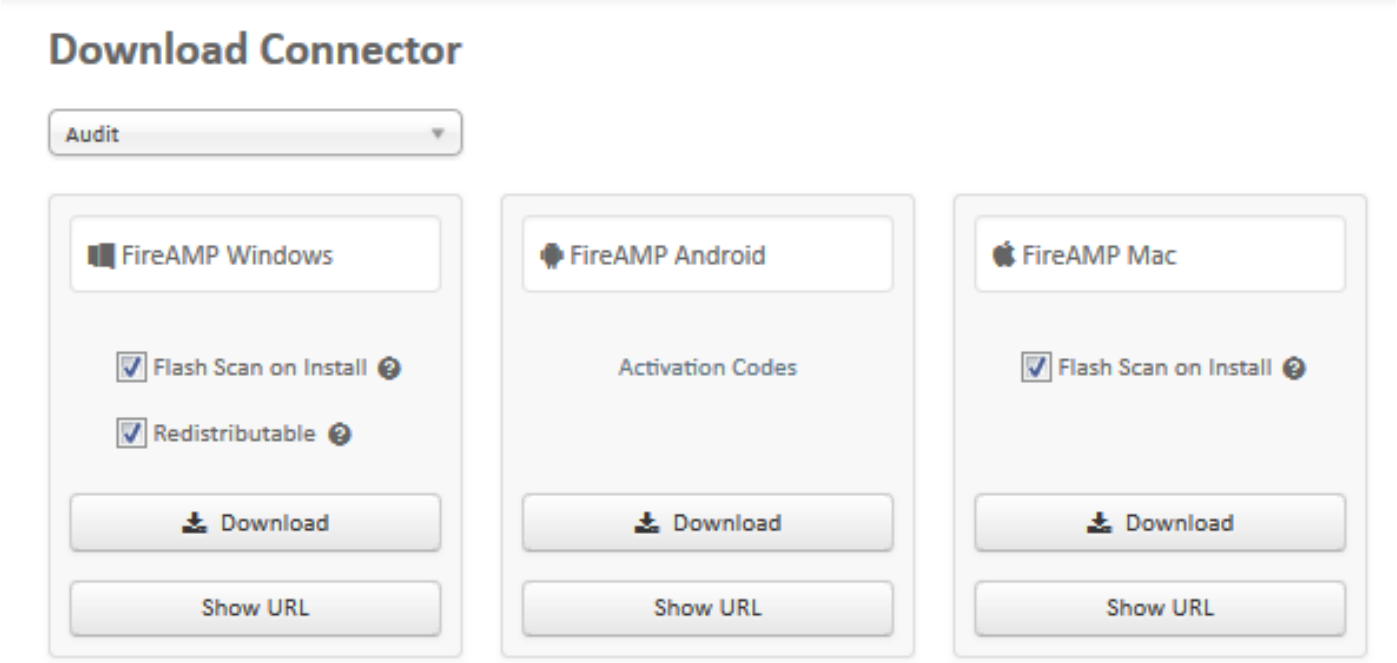
다운로드합니다. 이 실행 파일은 컴퓨터가 실행 중인 운영 체제가 32비트인지 아니면 64비트인지를 확인하고 적절한 FireAMP Connector 버전을 다운로드하여 설치합니다.

그러나 VPN을 사용하려면 재배포 가능 설치 프로그램을 다운로드하도록 선택해야 합니다. 이 설치 프로그램은 32비트 및 64비트 설치 프로그램이 모두 포함된 30MB 크기의 파일입니다. 이 파일은 네트워크 공유에 저장할 수도 있고, 여러 컴퓨터에 FireAMP Connector를 설치하기 위해 System Center Configuration Manager 등의 툴을 통해 그룹의 모든 컴퓨터로 푸시할 수도 있습니다. 부트스트래퍼 및 재배포 가능 설치 프로그램에는 설치용 컨피그레이션 파일로 사용되는 `policy.xml` 파일도 포함되어 있습니다.

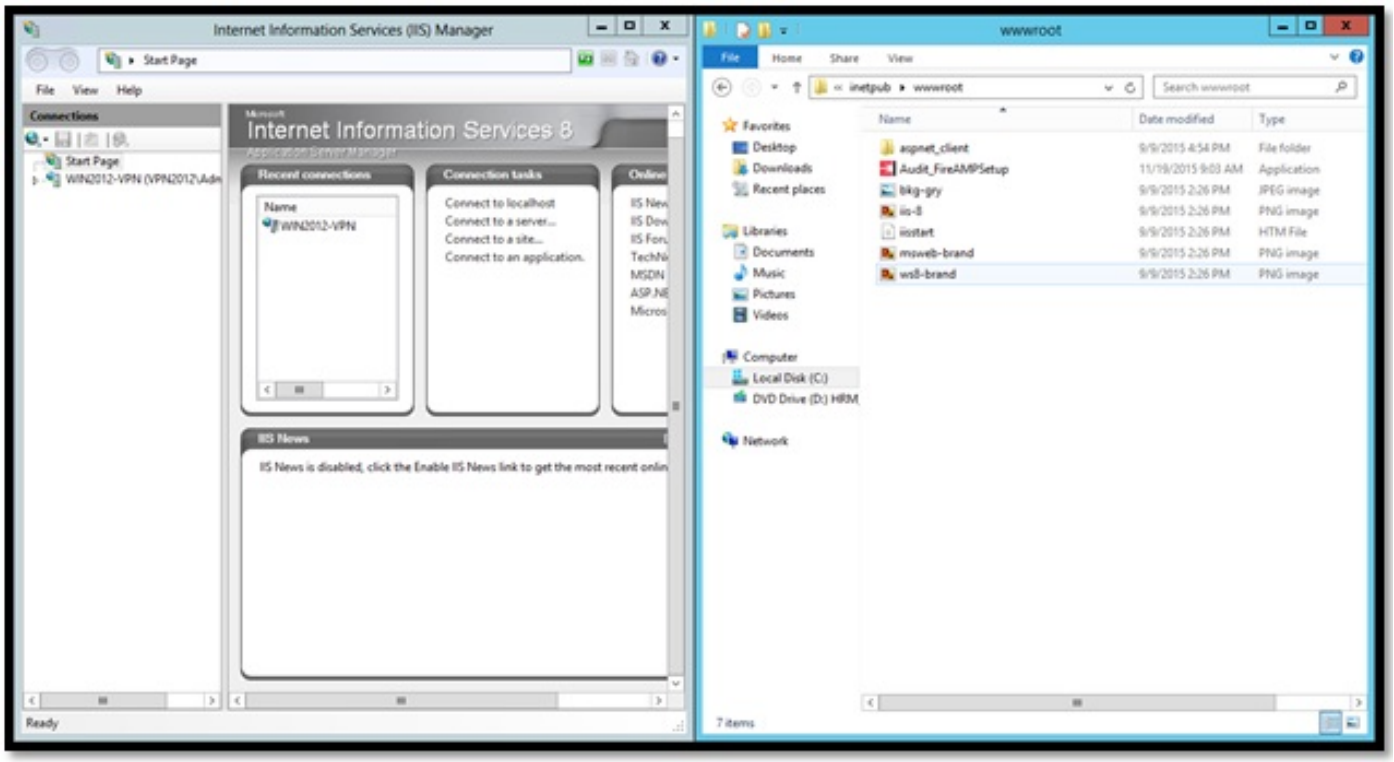
커넥터를 다운로드하려면 **Management(관리) > Download Connector(커넥터 다운로드)**로 이동합니다. 그런 다음, 유형을 선택하고 FireAMP **Download(다운로드)**(Windows, Android, Mac, Linux)를 선택합니다.



이 경우에는 **Download Connector(커넥터 다운로드)** 및 Windows 머신용 설치를 위해 **Audit(감사)** 옵션을 선택했습니다.



참고: 해당 파일을 다운로드하면 `.exe` 파일(이 예에서는 `Audit_FireAMPSetup.exe`)이 생성됩니다. 사용자가 AMP에 대한 컨피그레이션을 요청하는 경우, 해당 파일이 ASA에서 사용하고 다운로드할 수 있도록 웹 서버로 전송됩니다.

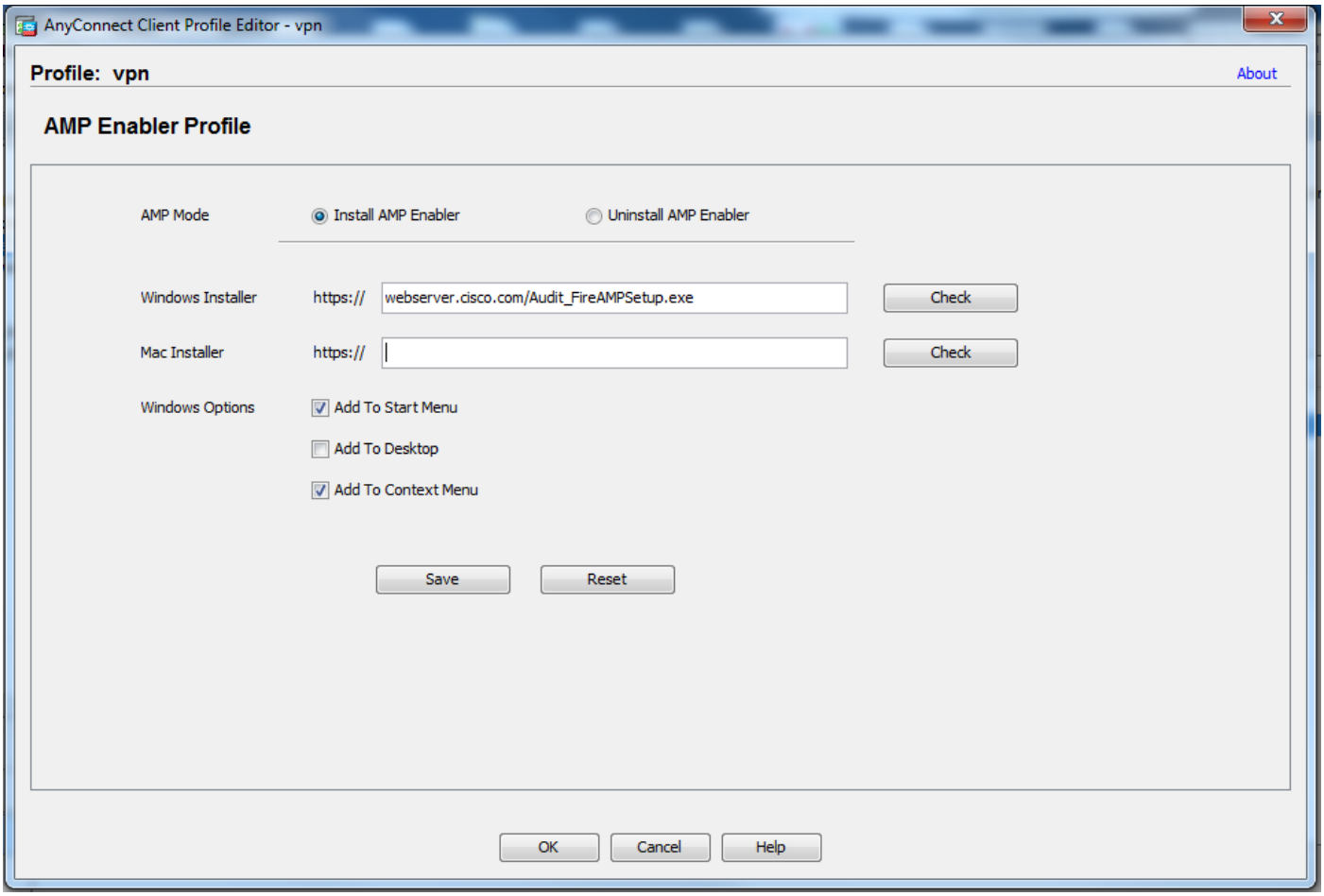


4단계: Web Security 클라이언트 프로파일 다운로드

전에 ASA(1단계)에서 생성된 AMP 프로파일로 돌아가 **AMP Enabler Profile(AMP Enabler 프로파일)**을 다음과 같이 수정합니다.

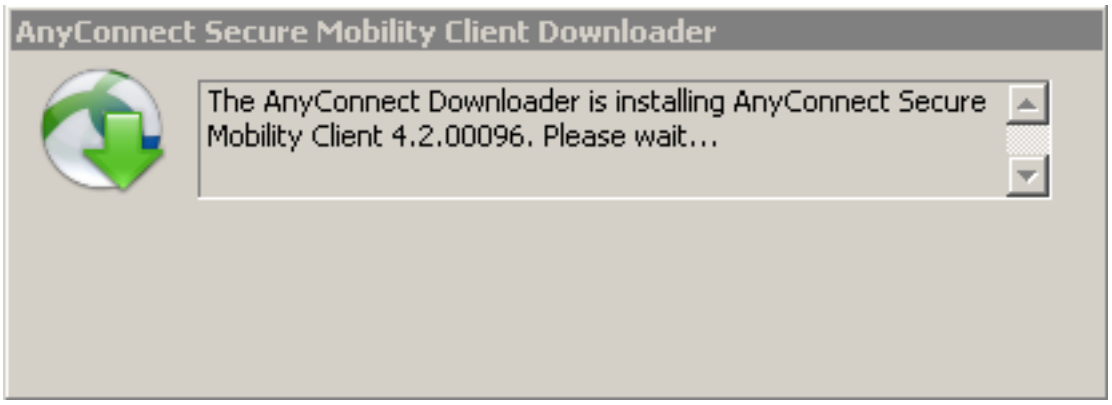
1. **AMP Mode(AMP 모드)**의 경우, **Install AMP Enabler(AMP Enabler 설치)**를 선택합니다.
2. **Windows Installer(Windows 설치 프로그램)** 필드에 웹 서버의 IP 및 FireAMP에 관한 파일을 추가합니다.
3. **Windows Options(Windows 옵션)**는 선택 사항입니다.

OK(확인)를 클릭하여 변경 사항을 적용합니다.



5단계: AnyConnect에 연결하여 모듈 설치 확인

AnyConnect VPN 사용자가 연결할 경우, ASA는 VPN을 통해 AnyConnect AMP Enabler 모듈을 푸시합니다. 이미 로그인되어 있는 사용자의 경우, 이 기능을 사용하려면 로그오프한 후 다시 로그인하는 것이 좋습니다.

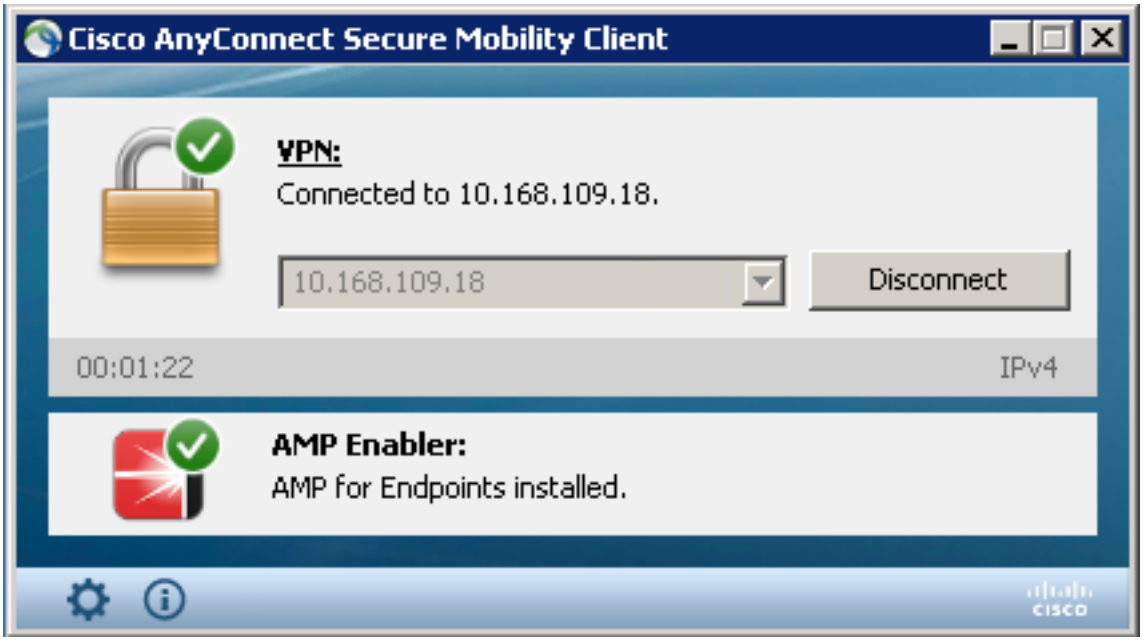


6단계: VPN 연결 및 AMP Enabler 확인

VPN이 연결되었고 **AMP Enabler**가 웹 서버에서 컨피그레이션을 수집하는지 확인합니다.

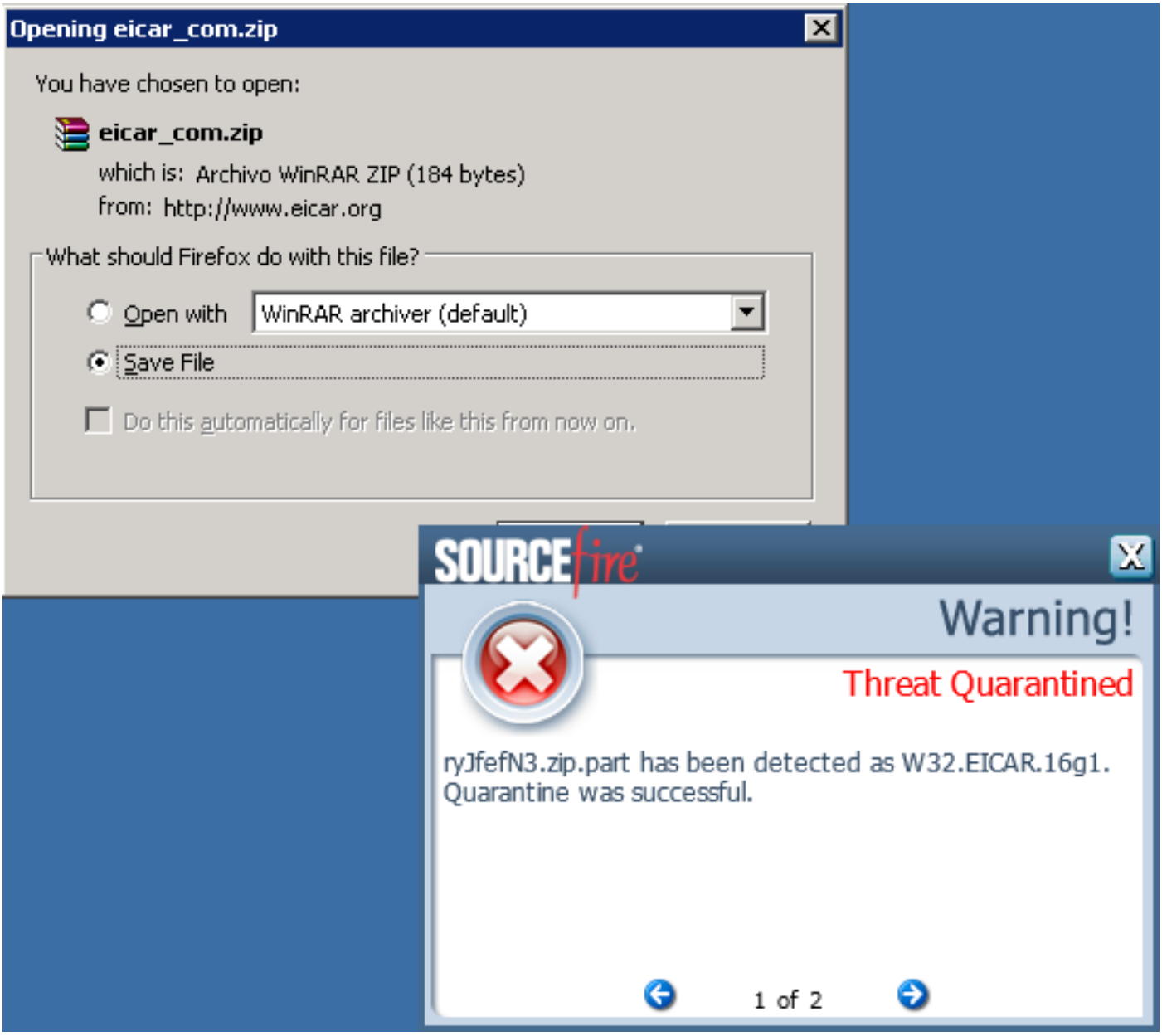
7단계: AnyConnect를 검사하여 모두 설치되었는지 확인

일단 VPN이 연결되었고 웹 서버에서 수집한 컨피그레이션이 설치되면 AnyConnect를 확인하고 모두 제대로 설치되었는지 확인합니다.



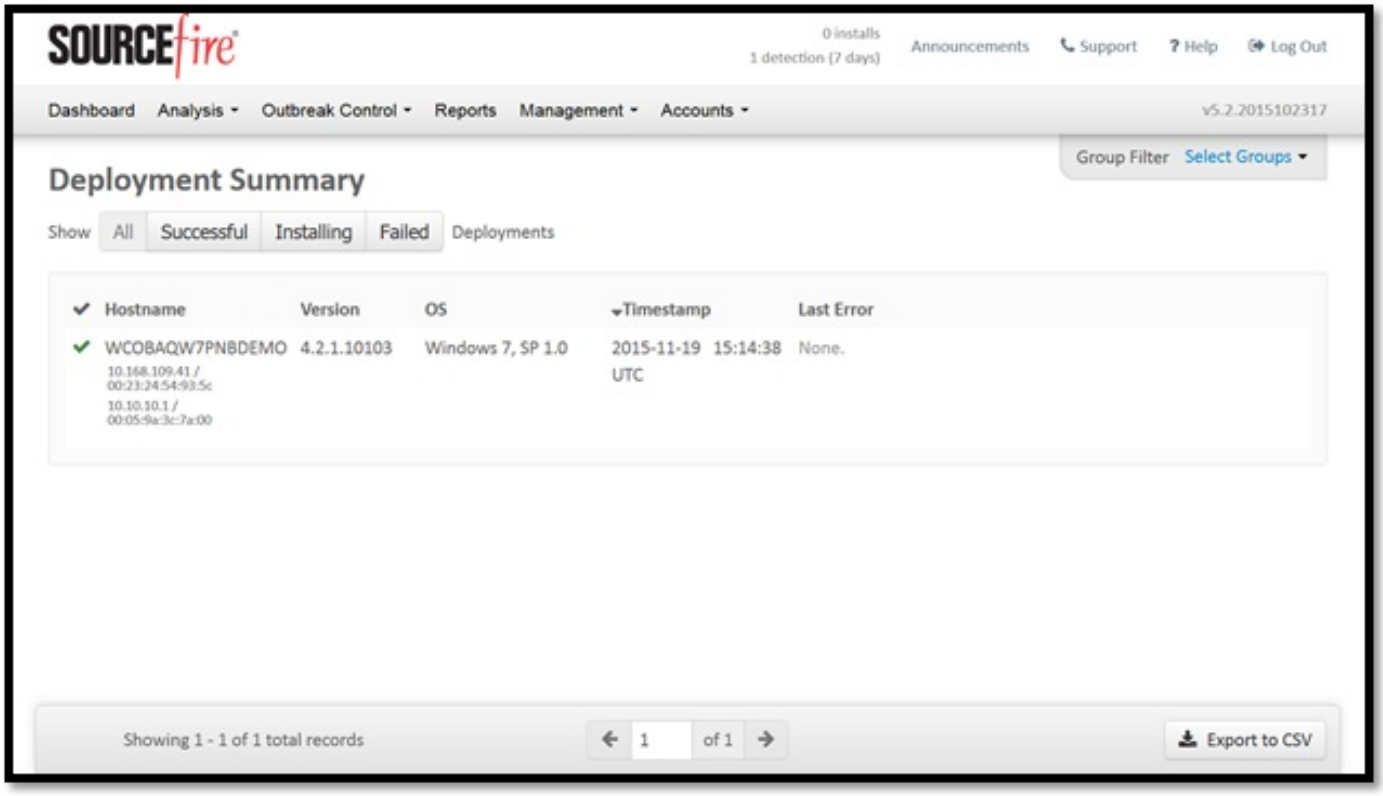
8단계: 컴퓨터에서 zip 파일에 포함된 Eicar 문자열로 테스트

컴퓨터에서 zip 파일에 포함된 Eicar 문자열로 테스트하여 모두 예상대로 작동하는지 확인합니다.



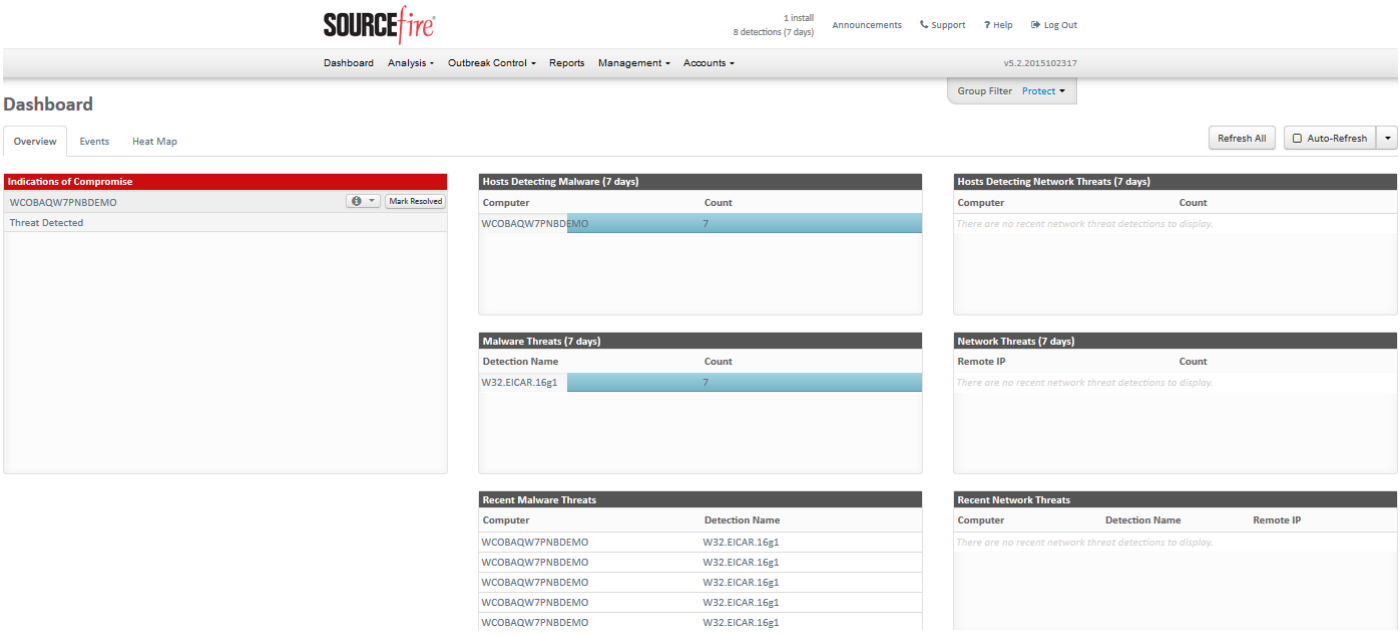
9단계: 구축 요약

이 페이지에는 FireAMP Connector 설치 성공 및 실패 목록과 현재 진행 중인 설치 목록이 표시됩니다. **Management(관리) > Deployment Summary(구축 요약)**로 이동할 수 있습니다.



10단계: 스레드 탐지 확인

이 페이지에는 FireAMP Connector에서 차단한 스레드 목록 및 영향을 받은 머신 목록도 표시됩니다. **Dashboard(대시보드)**로 이동할 수 있습니다.



추가 정보

FireAMP Windows Connector와 호환되지 않는 소프트웨어:

1. Check Point의 Zone Alarm
2. Carbon Black
3. Res Software AppGuard

관련 문서

- AMP Enabler 구성