

Installation und Konfiguration des AMP-Moduls über AnyConnect 4.x und AMP Enabler

Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[AnyConnect-Bereitstellung für AMP Enabler durch ASA](#)

[Schritt 1: Konfigurieren des AnyConnect AMP Enabler Client-Profiles](#)

[Schritt 2: Bearbeiten Sie die Gruppenrichtlinie, um den AnyConnect AMP Enabler herunterzuladen.](#)

[Schritt 3: Laden Sie die FireAMP-Richtlinie herunter](#)

[Schritt 4: Laden Sie das Web Security Client-Profil herunter](#)

[Schritt 5: Herstellen einer Verbindung mit AnyConnect und Überprüfen der Installation des Moduls](#)

[Schritt 6: Starten der VPN-Verbindung Installation von AMP Enabler und AMP-Anschluss](#)

[Schritt 7: Überprüfen Sie AnyConnect, und überprüfen Sie, ob alles installiert ist.](#)

[Schritt 8: Testen mit einer in einer Zombies-PDF-Datei enthaltenen Zeichenfolge](#)

[Schritt 9: Bereitstellungsübersicht](#)

[Schritt 10: Überprüfung der Threaderkennung](#)

[Zusätzliche Informationen](#)

[Zugehörige Informationen](#)

Einführung

In diesem Dokument werden Schritte zur Installation des AMP-Connectors (Advanced Malware Protection) mit AnyConnect beschrieben.

Der AnyConnect AMP Enabler wird als Medium zur Bereitstellung von AMP für Endgeräte verwendet. Sie selbst ist nicht in der Lage, die Einstufung einer Datei zu verurteilen. Die AMP für Endgeräte wird von der ASA an ein Endgerät übergeben. Nach der Installation von AMP nutzt es die Cloud-Kapazität, um die Einstufung von Dateien zu überprüfen. Ein weiterer AMP-Service kann Dateien zur dynamischen Analyse mit dem Namen ThreatGrid senden, um das Verhalten unbekannter Dateien zu bewerten. Diese Dateien können als schädlich eingestuft werden, wenn bestimmte Artefakte beachtet werden. Dies ist bei Zero-Day-Angriffen weit verbreitet.

Voraussetzungen

Anforderungen

- AnyConnect Secure Mobility Client Version 4.x
- FireAMP/AMP für Endgeräte
- Adaptive Security Device Manager (ASDM) Version 7.3.2 oder höher

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Adaptive Security Appliance (ASA) 5525 mit Softwareversion 9.5.1
- AnyConnect Secure Mobility Client 4.2.00096 unter Microsoft Windows 7 Professional 64-Bit
- ASDM-Version 7.5.1(112)

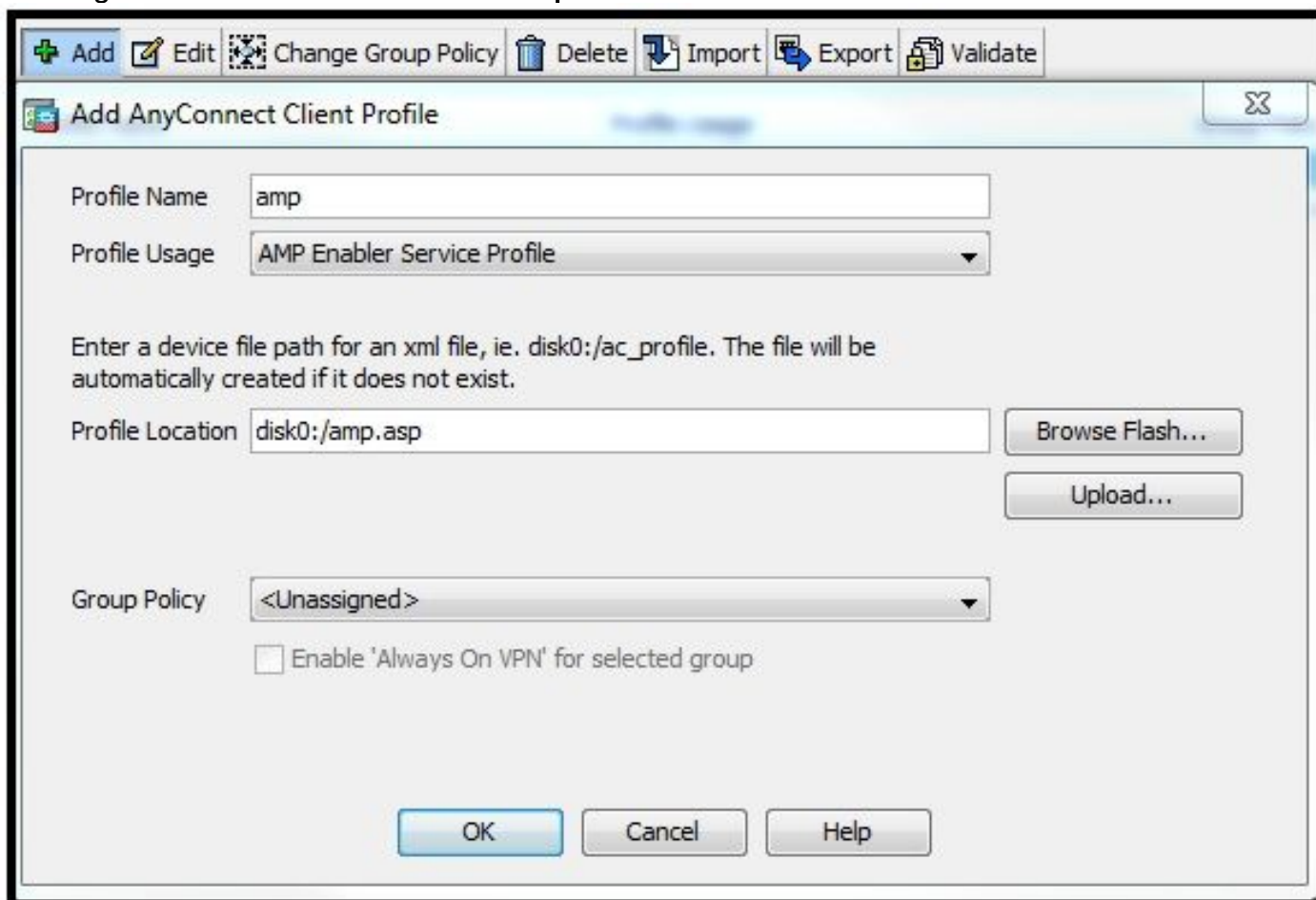
AnyConnect-Bereitstellung für AMP Enabler durch ASA

Die Konfiguration umfasst folgende Schritte:

- Konfigurieren Sie das Client-Profil von AnyConnect AMP Enabler.
- Bearbeiten Sie die AnyConnect VPN-Gruppenrichtlinie, und laden Sie das AMP Enabler-Serviceprofil herunter.
- Melden Sie sich beim AMP-Dashboard an, um den Link zum Download der Connector-URL zu erhalten.
- Überprüfen Sie die Installation auf dem Benutzercomputer.

Schritt 1: Konfigurieren des AnyConnect AMP Enabler Client-Profiles

- Navigieren Sie zu **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Client Profile**.
- Fügen Sie das **AMP Enabler-Serviceprofil** hinzu.



The screenshot shows the 'Add AnyConnect Client Profile' dialog box. The 'Profile Name' field contains 'amp'. The 'Profile Usage' dropdown is set to 'AMP Enabler Service Profile'. The 'Profile Location' field contains 'disk0:/amp.asp', with 'Browse Flash...' and 'Upload...' buttons to its right. The 'Group Policy' dropdown is set to '<Unassigned>'. There is an unchecked checkbox for 'Enable 'Always On VPN' for selected group'. At the bottom are 'OK', 'Cancel', and 'Help' buttons.

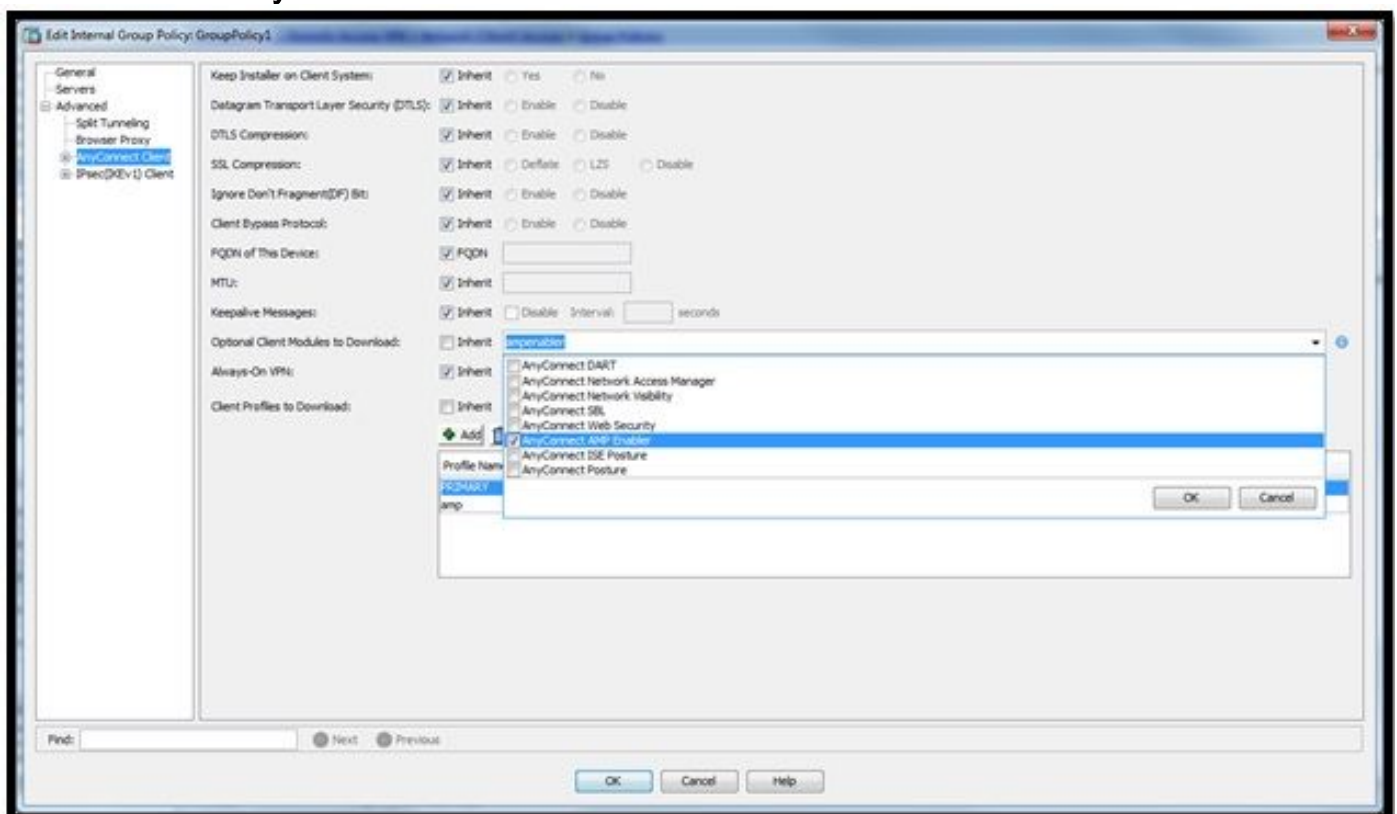
Profile Name	amp
Profile Usage	AMP Enabler Service Profile
Profile Location	disk0:/amp.asp
Group Policy	<Unassigned>

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

Schritt 2: Bearbeiten Sie die Gruppenrichtlinie, um den AnyConnect AMP Enabler herunterzuladen.

- Navigieren Sie zu **Konfiguration > Access VPN entfernen > Gruppenrichtlinien > Bearbeiten.**
- Gehen Sie zu **Erweitert > AnyConnect-Client > Optionale Client-Module**, um sie herunterzuladen.
- Wählen Sie **AnyConnect AMP Enabler** aus.



Schritt 3: Laden Sie die FireAMP-Richtlinie herunter

Hinweis: Bevor Sie fortfahren, prüfen Sie, ob Ihr System die Anforderungen für den Windows Connector für AMP der Endgeräte erfüllt.

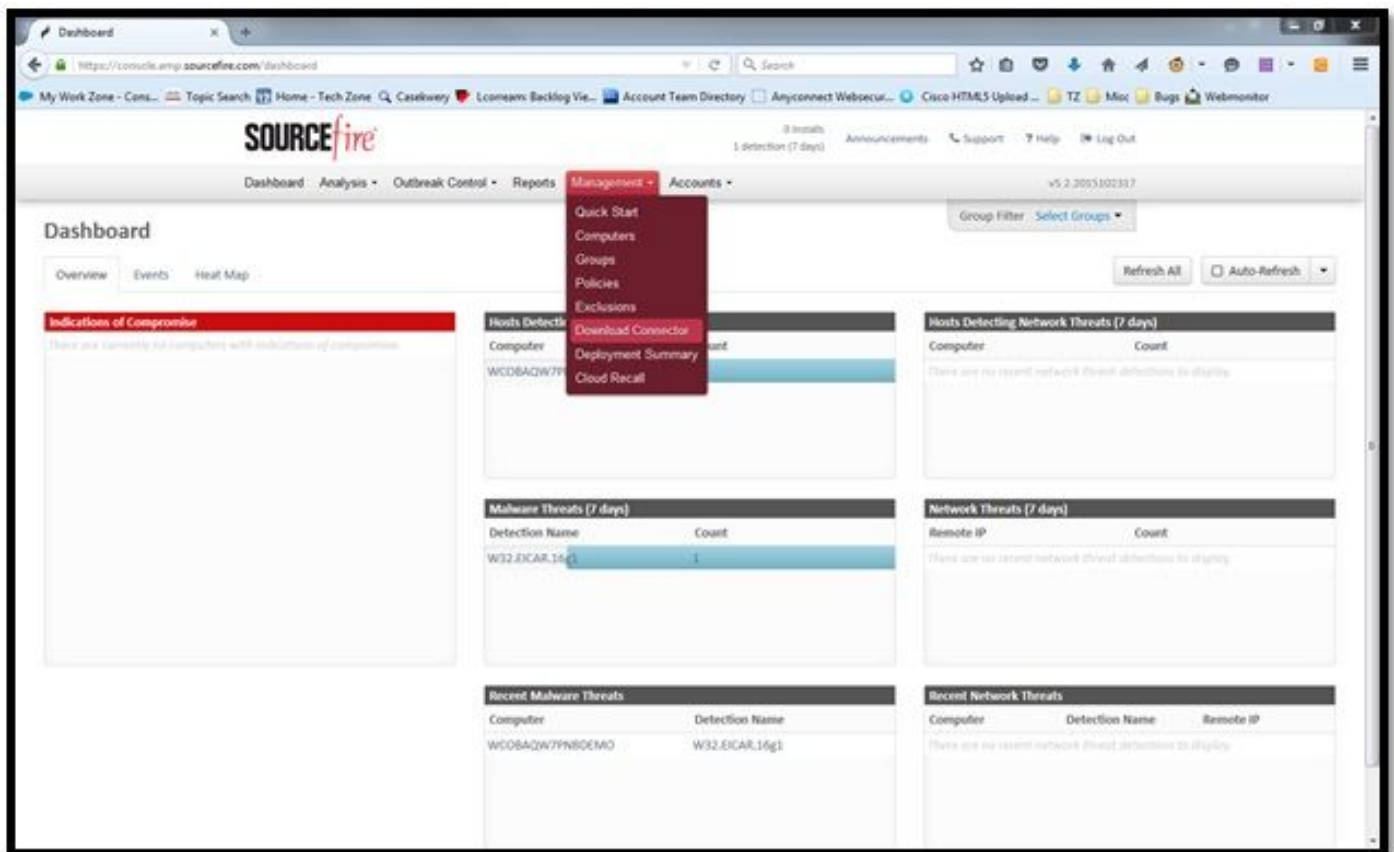
Systemanforderungen für AMP für Endgeräte Windows Connector

Dies sind die Mindestsystemanforderungen für den auf dem Windows-Betriebssystem basierenden FireAMP Connector. Der FireAMP Connector unterstützt sowohl 32-Bit- als auch 64-Bit-Versionen dieser Betriebssysteme. Die neueste AMP-Dokumentation ist in der [AMP-Bereitstellung](#) zu finden.

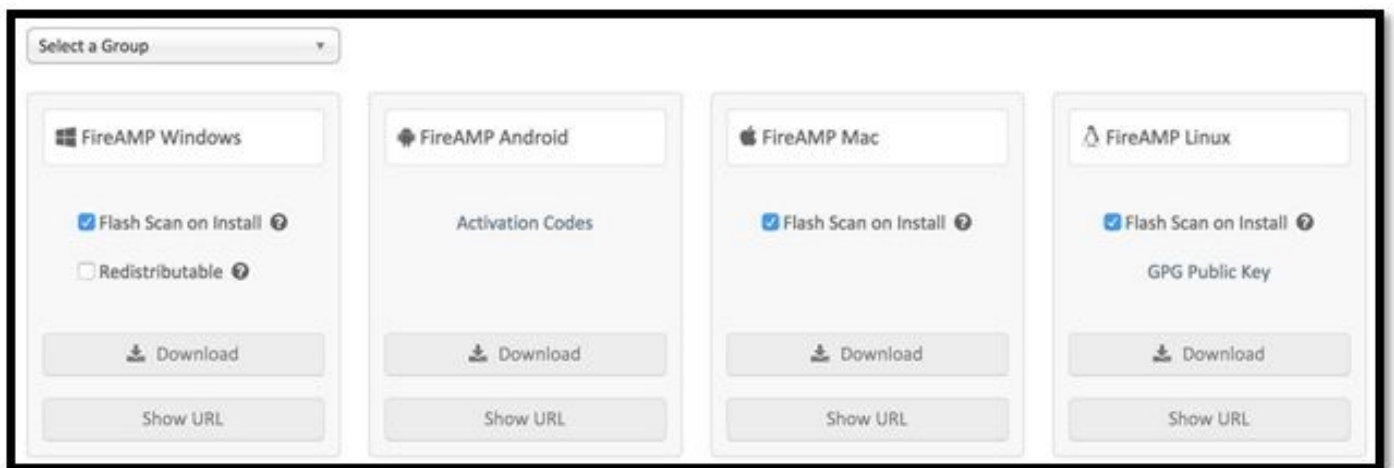
Betriebssystem	Prozessor	Arbeitsspeicher	Speicherplatz, Reiner Cloud-Modus	Festplattenspeicher
Microsoft Windows 7	Prozessor mit 1 GHz oder schneller	1 GB RAM	150 MB freier Festplattenspeicher - nur Cloud-Modus	1 GB freier Festplattenspeicher - TETRA
Microsoft Windows 8 und 8.1 (erfordert FireAMP Connector 5.1.3 oder höher)	Prozessor mit 1 GHz oder schneller	512 MB RAM	150 MB freier Festplattenspeicher - nur Cloud-Modus	1 GB freier Festplattenspeicher - TETRA
Microsoft Windows Server 2003	Prozessor mit 1 GHz oder schneller	512 MB RAM	150 MB freier Festplattenspeicher - nur Cloud-Modus	1 GB freier Festplattenspeicher - TETRA
Microsoft Windows Server 2008	Prozessor ab 2 GHz	2 GB RAM	150 MB verfügbarer Festplattenspeicher - nur Cloud-Modus	1 GB freier Festplattenspeicher - TETRA
Microsoft Windows Server 2012 (erfordert FireAMP Connector 5.1.3 oder höher)	Prozessor ab 2 GHz	2 GB RAM	150 MB verfügbarer Festplattenspeicher - nur Cloud-Modus	1 GB freier Festplattenspeicher - TETRA

Am häufigsten wird das AMP-Installationsprogramm auf dem Enterprise-Webserver platziert.

Um den Connector herunterzuladen, navigieren Sie zu **Management > Download Connector (Management > Connector herunterladen)**. Wählen Sie dann Typ und **Download FireAMP** (Windows, Android, Mac, Linux).



Auf der Seite Download Connector (Anschluss herunterladen) können Sie die Installationspakete für jeden FireAMP-Connector-Typ herunterladen. Dieses Paket kann auf einer Netzwerkfreigabe platziert oder über Managementsoftware verteilt werden.



Gruppe auswählen

- **Nur Audit:** Überwachen des Systems auf Grundlage von SHA-256, berechnet über jede Datei. Dieser Modus "Audit only" (Nur Prüfung) isoliert die Malware nicht, sendet aber ein Ereignis als Warnung.
- **Schutz:** Schützen Sie den Modus durch Quarantäne schädlicher Dateien. Überwachen Sie das Kopieren und Verschieben von Dateien.
- **Triage:** Diese Funktion ist für den Einsatz auf bereits kompromittierten/infizierten Computern vorgesehen.
- **Server:** Installations-Suite für Windows-Server, wo der Anschluss ohne Tetra-Engine und DFC-Treiber installiert wird. Diese Gruppe ist nach ihrem Namen für Controller-Server

konzipiert, die keine Domänen sind.

- **Domänencontroller:** Die Standardrichtlinie für diese Gruppe ist auf den Überwachungsmodus wie in der Servergruppe festgelegt. Ordnen Sie alle Active Directory-Server in dieser Gruppe zu, d. h. der Connector wird auf einem Windows Domain Controller ausgeführt.

Die AMP verfügt über die Funktion TETRA, die vollständige Antivirus-Engine ist. Diese Option ist für jede Richtlinie optional.

Funktionen

- **Flash Scan bei Installation:** Der Scan-Prozess wird während der Installation ausgeführt. Es ist relativ schnell und wird empfohlen, nur einmal auszuführen.
- **Weitervertrieb:** Sie sollten ein einziges Paket herunterladen, das 32-Bit- und 64-Bit-Installationsprogramme enthält. Statt eines Bootstrappers, der verfügbar ist, bleibt diese Option deaktiviert und lädt die Installer-Dateien nach der Ausführung.

Hinweis: Sie können eine eigene Gruppe erstellen und zugeordnete Richtlinien konfigurieren. Der Zweck besteht darin, alle z. B. Active Directory-Server in einer Gruppe zu platzieren, in der sich die Richtlinie im Überwachungsmodus befindet.

Der Bootstrapper und das verteilbare Installationsprogramm enthalten auch eine policy.xml-Datei, die als Konfigurationsdatei für den AMP-Anschluss verwendet wird.

Schritt 4: Laden Sie das Web Security Client-Profil herunter

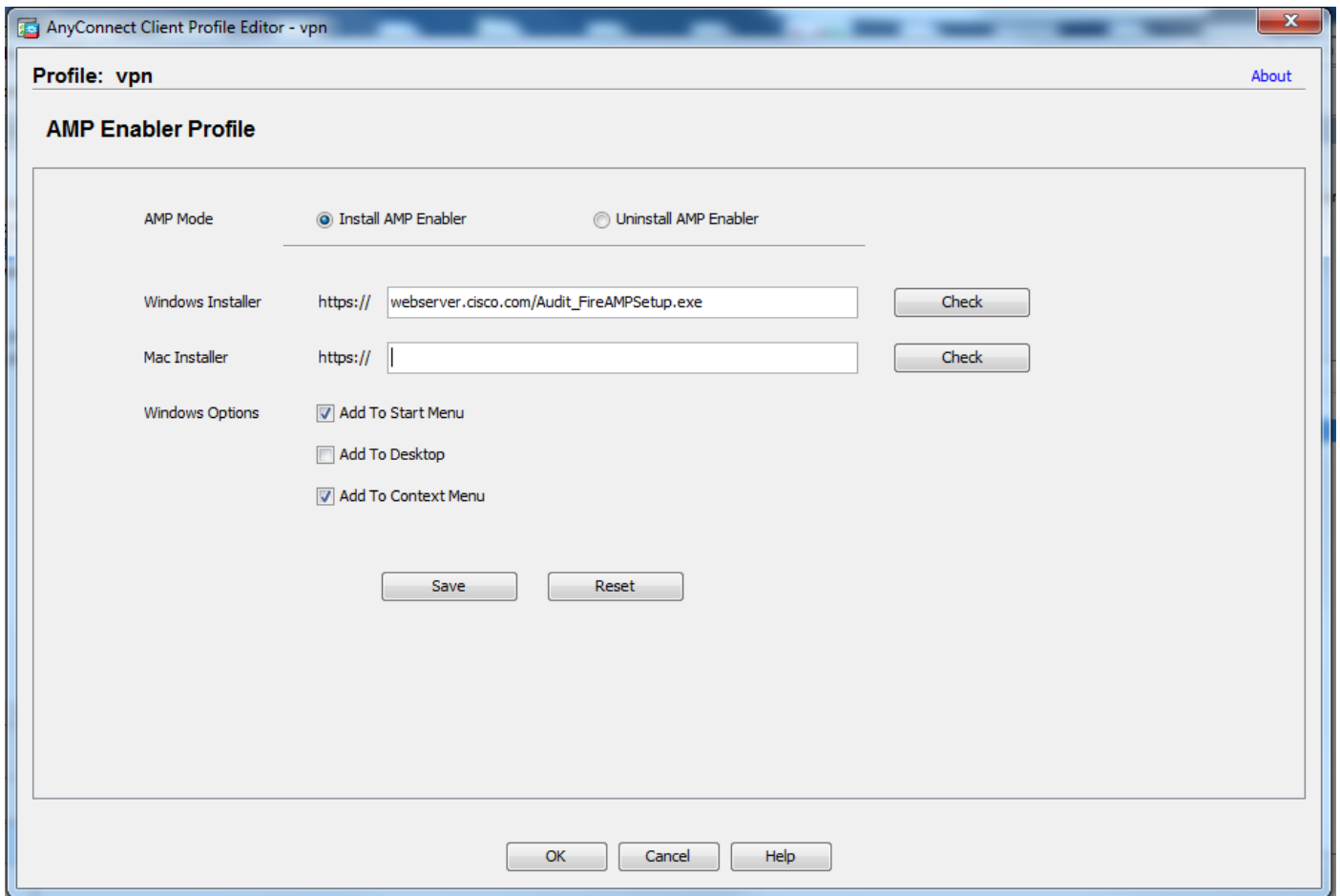
Geben Sie einen Firmen-Webserver oder eine Netzwerkfreigabe mit dem AMP-Installationsprogramm an. Diese Methode wird in der Regel von verschiedenen Unternehmen verwendet, um Bandbreite zu sparen und vertrauenswürdige Installationsprogramme an einem zentralen Ort zu platzieren.

Stellen Sie sicher, dass der HTTPS-Link auf den Endpunkten ohne Zertifikatfehler erreicht werden kann und dass das Root-Zertifikat im Computerspeicher installiert ist.

Wechseln Sie zurück zum zuvor auf der ASA erstellten AMP-Profil (Schritt 1), und bearbeiten Sie das **AMP Enabler-Profil**:

1. Klicken Sie für den AMP-Modus auf das Optionsfeld **AMP Enabler installieren**.
2. Fügen Sie im Feld **Windows Installer** die IP für den Webserver und die Datei für FireAMP hinzu.
3. Windows-Optionen sind optional.

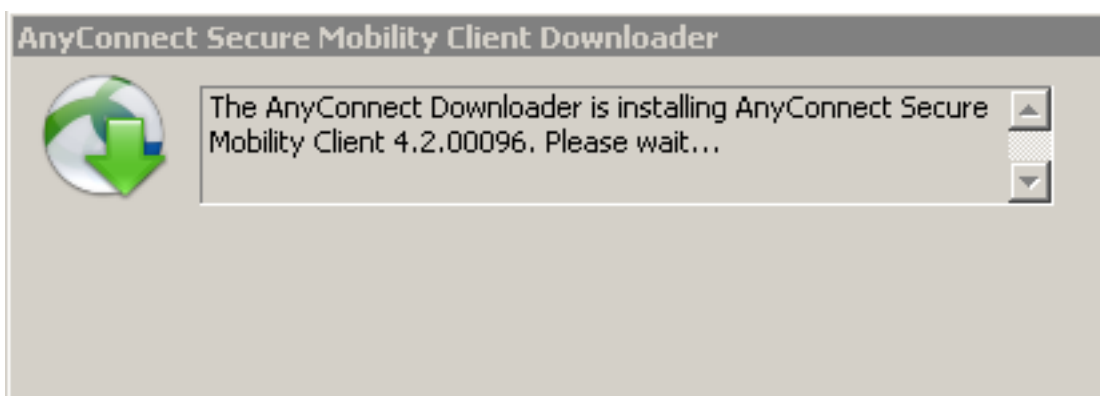
Klicken Sie auf **OK**, und übernehmen Sie die Änderungen.



Schritt 5: Herstellen einer Verbindung mit AnyConnect und Überprüfen der Installation des Moduls

Wenn AnyConnect VPN-Benutzer eine Verbindung herstellen, leitet ASA das AnyConnect AMP Enabler-Modul über das VPN weiter. Für bereits angemeldete Benutzer wird empfohlen, sich abzumelden und sich dann wieder anzumelden, damit die Funktion aktiviert werden kann.

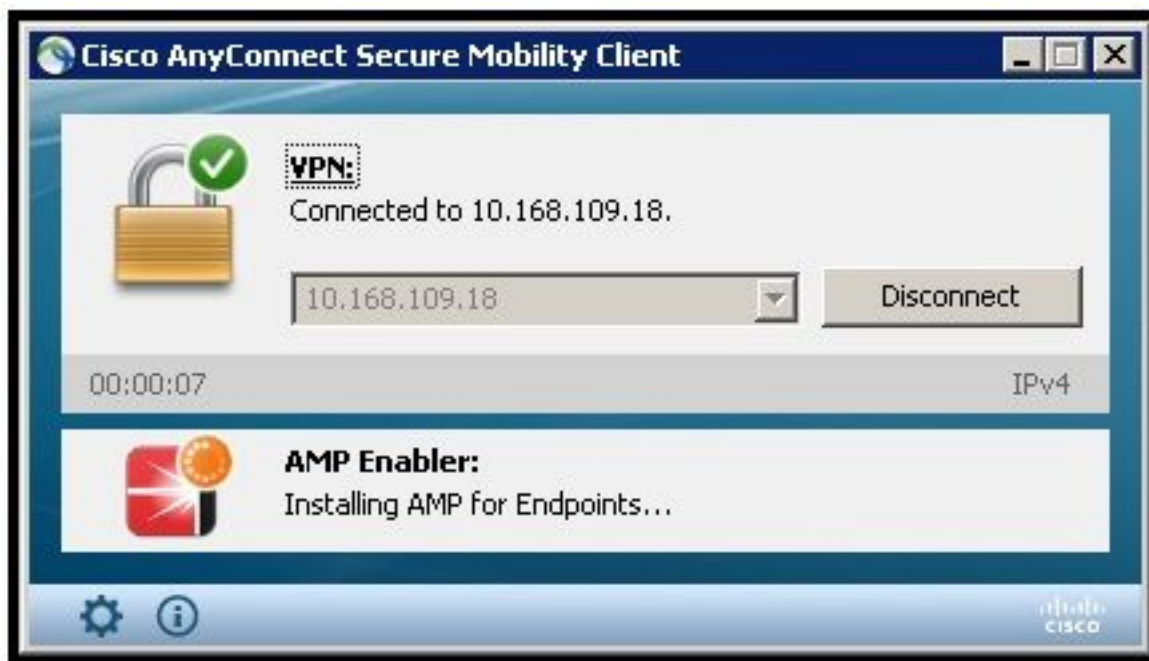
```
10:08:29 AM    Establishing VPN session...
10:08:29 AM    The AnyConnect Downloader is performing update checks...
10:08:29 AM    Checking for profile updates...
10:08:29 AM    Checking for product updates...
10:08:31 AM    Downloading AnyConnect AMP Enabler 4.4.01054 - 48%
10:08:32 AM    Downloading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



Schritt 6: Starten der VPN-Verbindung Installation von AMP Enabler und AMP-

Anschluss

Wenn Sie auf die Schaltfläche Verbinden klicken, um das VPN zu starten, wird das neue Downloader-Modul heruntergeladen. AMP Enabler wird aktiviert und lädt das AMP-Paket von dem URL-Pfad herunter, den Sie zuvor einige Schritte angegeben haben.



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]

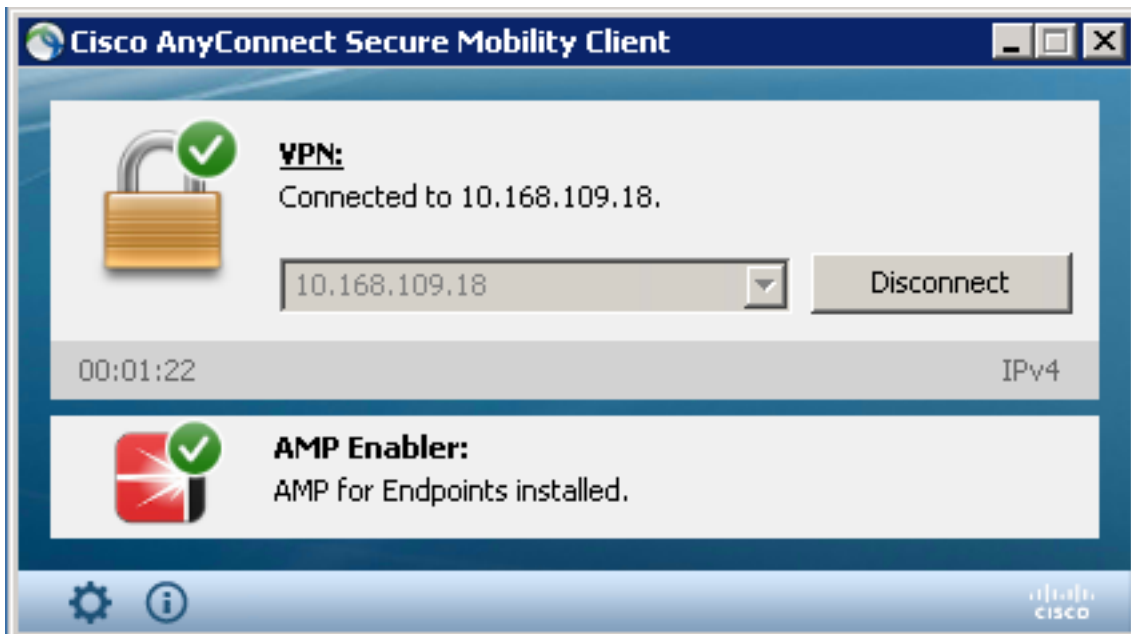
Schritt 7: Überprüfen Sie AnyConnect, und überprüfen Sie, ob alles installiert ist.

Wenn das VPN verbunden ist und die Konfiguration des Webserver installiert ist, aktivieren Sie AnyConnect, und überprüfen Sie, ob alle Komponenten ordnungsgemäß installiert sind.

In services.msc finden Sie einen neuen Service mit dem Namen CiscoAMP_5.1.3. Im Powershell-Befehl wird Folgendes angezeigt:

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

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



Der AMP Installer fügt dem Windows-Betriebssystem neue Treiber hinzu. Sie können den Befehl driverquery verwenden, um die Treiber aufzulisten.

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

```

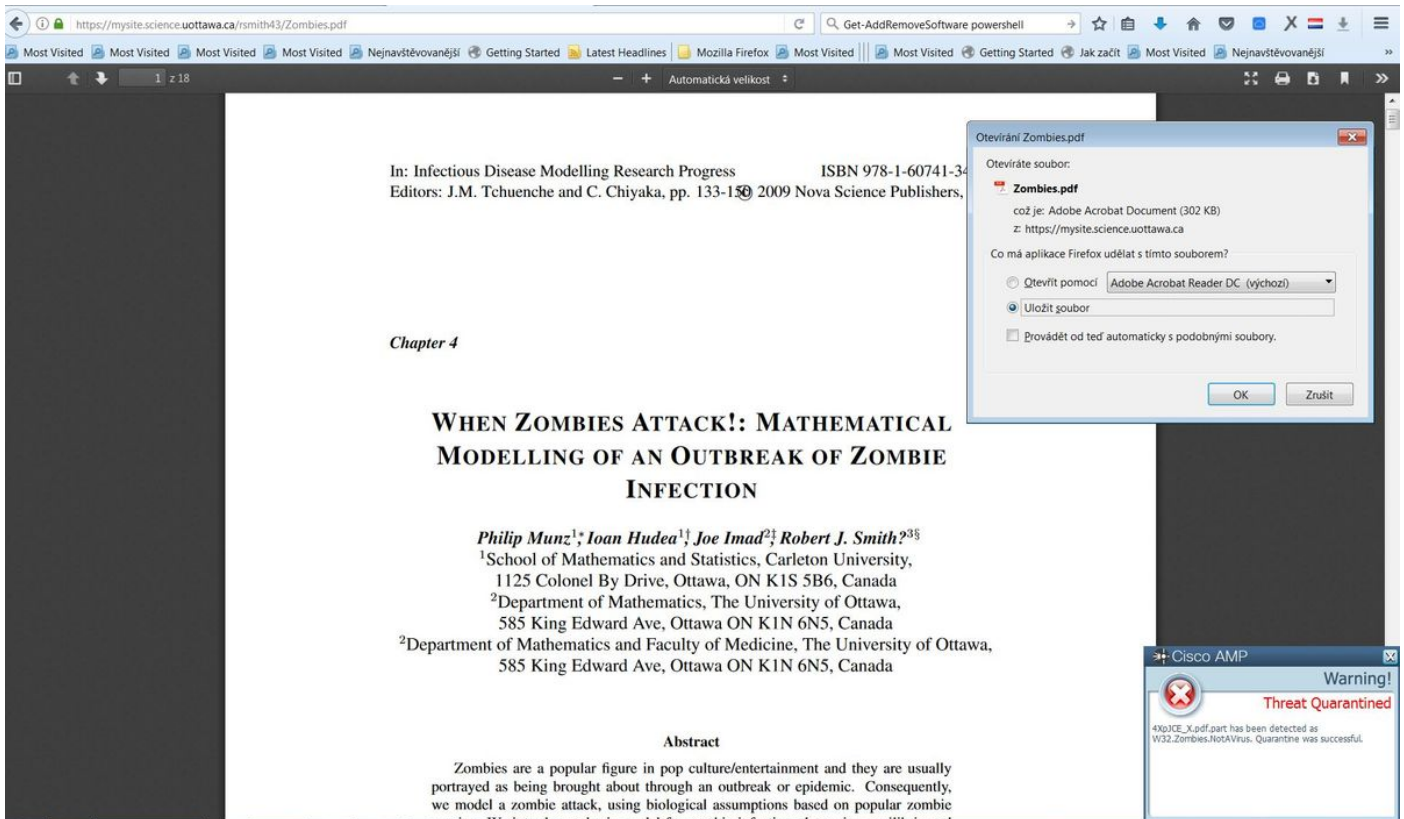
ImmunetProte ImmunetProtectDriver  ImmunetProtectDriver  File System  System  Running
OK          TRUE          FA
LSE         4,096         69,632         0         3/17/2017 5:04:20 PM
\??\C:\WINDOWS\System32\Drivers\immunetprotect.s 8,192

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

```

Schritt 8: Testen mit einer in einer Zombies-PDF-Datei enthaltenen Zeichenfolge

Testen Sie mit einer Eicar-Zeichenfolge, die in einer Zombies-PDF-Datei auf einem Testcomputer enthalten ist, um zu überprüfen, ob die schädliche Datei unter Quarantäne gestellt wurde.



Zombies.pdf enthält eine Zeichenkette

Schritt 9: Bereitstellungsübersicht

Auf dieser Seite finden Sie eine Liste der erfolgreichen und fehlgeschlagenen FireAMP-Connectors, die derzeit installiert sind. Sie können zu **Management > Deployment Summary** wechseln.

✓ 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.

Schritt 10: Überprüfung der Threaderkennung

Zombies.pdf löste ein Quarantäne-Ereignis aus und schickte es an das AMP-Dashboard.

The screenshot shows the Cisco AMP for Endpoints dashboard. At the top, there is a navigation bar with 'Dashboard', 'Analysis', 'Outbreak Control', 'Reports', 'Management', and 'Accounts'. A notification banner for 'New AMP for Endpoints Linux Connector' is visible. The main dashboard area has tabs for 'Dashboard', 'Inbox', 'Overview', 'Events', and 'Heat Map'. A filter section allows for selecting event types and groups. The main content area displays a quarantine event for a file named '4XpjCE_X.pdf.part' detected as 'W32.Zombies.NotAVirus'. The event details include the detection time (2017-07-27 13:32:08 UTC), the file's SHA-256 fingerprint, filename, filepath, file size (309500 bytes), parent fingerprint, and parent filename ('firefox.exe'). Action buttons for 'Report', 'Restore File', and 'All Computers' are present at the bottom of the event details.

Quarantäne-Ereignis

Zusätzliche Informationen

Um Ihr AMP-Konto zu erhalten, können Sie sich für die ATS University anmelden. Sie erhalten eine Übersicht über die AMP-Funktionen in LAB.

Zugehörige Informationen

- [Konfigurieren von AMP Enabler](#)
- [Technischer Support und Dokumentation - Cisco Systems](#)