# 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-Profils 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-Profils

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

🕀 Add 🗹 Edi	🕅 Change Group Policy 📋 Delete 🌄 Import 🖶 Export 🗿 Va	lidate
🔁 Add AnyCo	nnect Client Profile	X
Profile Name	amp	
Profile Usage	AMP Enabler Service Profile	
Enter a devic automatically	e file path for an xml file, ie. disk0:/ac_profile. The file will be reated if it does not exist.	
Profile Locati	on disk0:/amp.asp	Browse Flash
		Upload
Group Policy	<pre></pre> <pre></pre> <pre></pre>	
	Enable 'Always On VPN' for selected group	
	OK Cancel Help	

🕈 Add 🗹 Edit 🞇 Change Group Polic	y 📋 Delete 🚯 Import 🖶 Exp	ort 🚮 Validate	
Profile Name	Profile Usage	Group Policy	Profile Location
RIMARY	AnyConnect VPN Profile	GroupPolicy1	disk0:/primary.xml
imp	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.

I souther the second second	THE R. L. LEWIS	-	20 Atl		
Keep Instater on Clenit Systems	(g) shelt	Tes	( No		
Detagram Transport Layer Security (DTLS):	V Inherit	O thatle	C Duble		
OTLS Compression:	2 Inherit	C Brable	O Double		
SSL Compression:	2 Inherit	🗇 Defete	0.125	C Dade	
Ignore Don't Fragment(DF) Siti	(2) Inherit	C Endle	🔿 Deable		
Client Bypass Protocol:	[] Inherit	() brable	() Double		
PQDN of This Device:	PQ0N			1	
MTU:	[2] Inherit				
Keepalive Messages:	(2) Inherit	Dealer	Solervin [	seconds	
Optional Client Modules to Download:	Elbheit	impenable	1		
Always-On VPN:	2 Inherit	AnyCon	nect DART	Access Manager	
Client Profiles to Doveload:	Dheit	AnyCan AnyCan	nect Network nect SIL	k visbility	
	4 Add 1	AnyCon	nect Web Sec	curity	
	Profile Nam	AnyCon	nect ISE Post nect Posture	fure	
	SEDMRY!			or	Cano
	100			homojim	anamad Approximity
Not      Prote					

### 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 <u>AMP-</u> <u>Bereitstellung</u> zu finden.

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

P Dathboard X +	-			- 0 ×
B   Https://conscie.org/sourcefine.com/deshidoord		v C Q Associ	2 A B	* * 4 0 • 0 = • 8 =
▶ My Work Zone - Cons 🚐 Topic Search 🛐 Home - Tech Zone 🔍 Casekwery ♥	Loomeans Backlog Vie 🔛 Acc	ount Team Directory 🗔 Anyconnect Websec	w 🗿 Cisce HTMLS Upleed 🧾	TZ 🍰 Mici 🎴 Bugs 🛕 Webmonitor
SOURCE		() Installs 1 Setection (7 days) Advisor	ncements Chapport 7 Help	IP Lig Out
Dashboard Analysis - Outbreak Con	stol - Reports Management	+ Accounts +	15	2.3055102317
Dashboard	Quick Start Computers		Group Filter Select	t Groups +
Overview Events Heat Map	Groups Policies			Refresh All O Auto-Refresh •
Indications of Compromise	Hosts Detectle Download C	annector 1	Hosts Detecting Network	Threats (7 days)
(These you cannotly not computery with total attum of computation	Computer Deployment	Summary unt	Computer	Count
	Cloud Recal			
				8
	Mahaare Threats (7 days)		Network Threats (7 days	
	Detection Name	Coant	Remote IP	Count
	W32-DCAR.35	1	There are no antend horizon	of the datasets in digits
	Recent Malware Threats		Recent Network Threats	
	Computer	Detection Name	Computer	Detection Name Remote IP
	modelm/modelW0	- WSZICHUMI, 1982		an anna an ann an Anna

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.

lect a Group *			
FireAMP Windows	FireAMP Android	SireAMP Mac	∆ FireAMP Linux
Flash Scan on Install Redistributable	Activation Codes	Flash Scan on Install Ø	GPG Public Key
🛓 Download	🛓 Download	🛓 Download	🛓 Download
Show URL	Show URL	Show URL	Show URL

#### 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.

AnyConnect Client Profile Editor	- vpn	X
Profile: vpn		About
AMP Enabler Profile		
AMP Mode	Install AMP Enabler     O Uninstall AMP Enabler	
Windows Installer	https:// webserver.cisco.com/Audit_FireAMPSetup.exe Check	
Mac Installer	https://	
Windows Options	☑ Add To Start Menu	
	Add To Desktop	
	☑ Add To Context Menu	
	Save Reset	
	OK Cancel Help	

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

### 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.

Cisco AnyCo	onnect Secure Mobility Client		_ 🗆 >
	<b>VPN:</b> Connected to 10.168.109.18.		
	10.168.109.18	<b>*</b>	Disconnect
00:00:07			IPv4
	AMP Enabler: Installing AMP for Endpoints		
<b>\$</b> ()			ajtajto cisco

If you look at the event viewer:

AMP enabler	ir	stall:									
Date	:	04/24/2017									
Time	:	10:08:34									
Туре	:	Information									
Source	:	acvpndownloader									
Description	:	Cisco AnyConnect	Secure	Mobility	Client	Downloader	(2)	exiting,	version	4.4.0105	54
, return cod	le	0 [0x0000000]									

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

Wenn das VPN verbunden ist und die Konfiguration des Webservers 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:\Us	ers\winUser348>	Get-	-Servio	ce -r	ıame	"*CiscoAMI	P*"	
Status	Name		Displa	ayNan	ne			
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>di	riverquery	/v   f	indstr immun	net			
ImmunetPro	te ImmunetP	rotectDrive	r Im	munetProtect	Driver	File System	System	Running
OK	TRUE	FA						
LSE	4,096	69,632	0	3/17/2017	5:04:20	PM		
\??\C:\WIN	DOWS\System	32\Drivers\	immune	tprotect.s 8	3,192			
ImmunetSel	fP ImmunetSe	elfProtectD	riv Im	munetSelfPro	tectDriv	/ File System	System	Running
OK	TRUE	FA						
LSE	4,096	28,672	0	3/17/2017	5:04:08	PM		
\??\C:\WIN	DOWS\System	32\Drivers\	immune	tselfprote 8	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.



Schritt 10: Überprüfung der Threaderkennung

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

	.amp.cisco.com/dashboard#/events/show/			CQ	Hledat			¥ ■ ▼	n o	• ^ =	- 1
st Visited 📓 Most Visite	ed 🧕 Most Visited 🧕 Most Visited 🧕	Nejnavštěvovanější 🖪 Getting Started 🌛 Latest Head	dlines 🧧 Mozilla Fi	refox 🧕 Most Visiti	ed 📗 🙆 Mos	Visited 🛞	Getting Started	🛞 Jak začít 📓 Most	Visited 🧕 N	Vejnavštěvovaněj	ŝí
	cisco AME	<sup>&gt;</sup> for Endpoints	•	Announcements	Support	<b>?</b> Help	Account	🕞 Log Out			
	Dashboard Analys	is 🗸 Outbreak Control 🗸 Reports Manageme	ent ~ Accounts ~		Search			Q			
	New AM Version 1.3.1	P for Endpoints Linux Connector 416 is now available. Learn more in the Official Relea	ase Notes	×							
ashboard	Consigner Frankling	0.00	anitive Incidents	2							
ashboard Inbox	Overview Events Heat Map	0 00	gniuve incidente	S							
- Filter: (New)  -								Se	lect a Filter		1
Event Type All	+	Group All Grou	sdr						+		
Filters Ad	ld filters by clicking on the T icon in the leek > Sort	rvent details						Not Subscribed	~ Reset	Save Filter A	s
DJANULIK-HYYPD.	cisco.com detected 4XpJCE_X.pdf.part a	s W32.Zombies.NotAVirus				P)	PP 100 Q	uarantine: Successful	2017-07	7-27 13:32:08 UT	C
DJANULIK-HYYPD.     File Detection	cisco.com detected 4XpJCE_X.pdf.part a	is W32.Zombies.NotAVirus				<b>P</b>		uarantine: Successful	2017-07	7-27 13:32:08 UT	TC
DJANULIK-HYYPD. File Detection Connector Info	cisco.com detected 4XpJCE_X.pdf.part a Detection Fingerprint (SHA-256)	s W32.Zombies.NotAVirus TW32.Zombies.NotAVirus T 00b32c34989bb002 O ~				Ph C		uarantine: Successful	2017-07	7-27 13:32:08 UT	гс
DJANULIK-HYYPD. File Detection Connector Info Comments	cisco.com detected 4XpjCE_X.pdf.part a Detection Fingerprint (SHA-256) Filename	s W32.Zombles.NotAVirus ▼W32.Zombles.NotAVirus ▼ 00b32c34989bb002				<b>P</b> P	29 <b>(C)</b> 9	uarantine: Successful	2017-07	7-27 13:32:08 UT	rc
DJANULIK-HYYPD. File Detection Connector Info Comments	cisco.com detected 4XpJCE,X.pdf.part a Detection Fingerprint (SHA-256) Filename Filepath	W32.Zombies.NotAVirus           TW32.Zombies.NotAVirus           T 00b32c34989bb002           T 4XpjCE_X.pdf.part           C:\Users\djanulik\AppData\Local\Temp\4XpjC	CE_X.pdf.part			(PP) (	₽₽ <b>(2</b> ) 9	uarantine: Successful	2017-07	7-27 13:32:08 UT	rc
DJANULIK-HYYPD. File Detection Connector Info Comments	clsco.com detected 4XpJCE,X.pdf.part a Detection Filename Filepath File Size (bytes)	TW32.Zombles.NotAVirus           TW32.Zombles.NotAVirus           T00b32c34989bb002           T4xpjCE_X.pdf.part           C:\Users\djanulik\AppData\Local\Temp\4XpjC           309500	CE_X.pdf.part			PP C	<b>₽₽ (Ω</b> ) Q	uarantine: Successful	2017-07	7-27 13:32:08 UT	гс
DJANULIK-HYYPD. File Detection Connector Info Comments	cisco.com detected 4XpJCE,X.pdf.part a Detection Filepartint (SHA-256) Fileparth Filepath File Size (bytes) Parent Fingerprint (SHA-256)	w32.Zombles.NotAVirus           T W32.Zombles.NotAVirus           T 00b32c34989bb002           T 4XpjCE_X.pdf.part           C:\Users\djanulik\AppData\Local\Temp\4XpjC           309500           T 0fff6b175fdf32be	CE_X.pdf.part			₽¥ [	90 ( <u>1</u>	uarantine: Successful	2017-07	-27 13:32:08 UT	rc
DJANULIK-HYYPD. File Detection Connector Info Comments	clsco.com detected 4XpJCE X.pdf.part a Detection Fingerprint (SHA-256) Filename Filepath File Size (bytes) Parent Fingerprint (SHA-256) Parent Filename	wW32.Zombles.NotAVirus           TW32.Zombles.NotAVirus           T00b32c34999bb002           T4XpJCE_X.pdf.part           C:\Users\djanulik\AppData\Local\Temp\4XpJC           309500           T0fff6b175fdf32be           Tfirefox.exe	CE_X.pdf.part			∎v C		uarantine: Successful	2017-07	-27 13:32:08 UT	rc

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