

Installation et configuration de module d'AMPÈRE par AnyConnect 4.x et Enabler d'AMPÈRE

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Composants utilisés](#)

[Déploiement d'AnyConnect pour l'Enabler d'AMPÈRE par l'ASA](#)

[Étape 1 : Configurez le profil de client d'Enabler d'AMPÈRE d'AnyConnect](#)

[Étape 2 : Éditez la stratégie de groupe pour télécharger l'Enabler d'AMPÈRE d'AnyConnect](#)

[Étape 3 : Téléchargez la stratégie de FireAMP](#)

[Étape 4 : Téléchargez le profil de client de sécurité Web](#)

[Étape 5 : Connectez à AnyConnect et vérifiez l'installation du module](#)

[Étape 6 : Vérifiez la connexion VPN et l'Enabler d'AMPÈRE](#)

[Étape 7 : Vérifiez AnyConnect et le vérifiez si tout est installé](#)

[Étape 8 : Test avec une chaîne d'Eicar contenue dans un fichier zip dans un ordinateur](#)

[Étape 9 : Résumé de déploiement](#)

[Étape 10 : Vérification de détection de thread](#)

[Informations supplémentaires](#)

[Informations connexes](#)

Introduction

Ce document décrit la méthode pour installer et configurer le module avancé de protection de malware (AMPÈRE) sur un système d'utilisateur avec AnyConnect.

L'Enabler d'AMPÈRE d'AnyConnect est utilisé comme support pour déployer l'AMPÈRE pour des points finaux. Il pousse l'AMPÈRE pour le logiciel de points finaux à un sous-ensemble de points finaux d'un serveur hébergé localement au sein de l'entreprise et installe des services d'AMPÈRE sur sa base de clients existante. Cette approche fournit à des administrateurs de base de clients d'AnyConnect un agent de Sécurité supplémentaire qui détecte les menaces potentielles de malware qui se produisent dans le réseau, retire ces menaces, et protège l'entreprise contre la compromission. Il épargne la bande passante et le temps pris pour télécharger, n'exige aucune modification du côté portail, et peut être fait sans qualifications d'authentification étant envoyées aux points finaux.

Conditions préalables

Conditions requises

- Version du client sécurisée 4.x de mobilité d'AnyConnect

- FireAMP/AMPÈRE pour des points finaux
- AnyConnect plus/permis d'apex
- Version 7.3.2 ou ultérieures d'Adaptive Security Device Manager (ASDM)

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Appliance de sécurité adaptable (ASA) 5525 avec la version de logiciel 9.5.1
- Client sécurisé 4.2.00096 de mobilité d'AnyConnect sur Microsoft Windows 7 64-bit professionnels
- Version 7.5.1(112) ASDM

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Déploiement d'AnyConnect pour l'Enabler d'AMPÈRE par l'ASA

Les étapes impliquées dans la configuration sont comme suit :

- Configurez le profil de client d'Enabler d'AMPÈRE d'AnyConnect.
- Éditez la stratégie de groupe VPN d'AnyConnect et téléchargez le service profile d'Enabler d'AMPÈRE.
- Éditez le profil d'AMPÈRE afin d'obtenir la configuration d'un web server.
- Vérifiez l'installation sur l'ordinateur d'utilisateur.

Étape 1 : Configurez le profil de client d'Enabler d'AMPÈRE d'AnyConnect

- Naviguez vers la configuration > l'Accès à distance VPN > réseau (client) Access > profil de client d'AnyConnect.
- Ajoutez le **service profile d'Enabler d'AMPÈRE**.

Add
 Edit
 Change Group Policy
 Delete
 Import
 Export
 Validate

Add AnyConnect Client Profile

Profile Name:

Profile Usage:

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:

Group Policy:

Enable 'Always On VPN' for selected group

Add
 Edit
 Change Group Policy
 Delete
 Import
 Export
 Validate

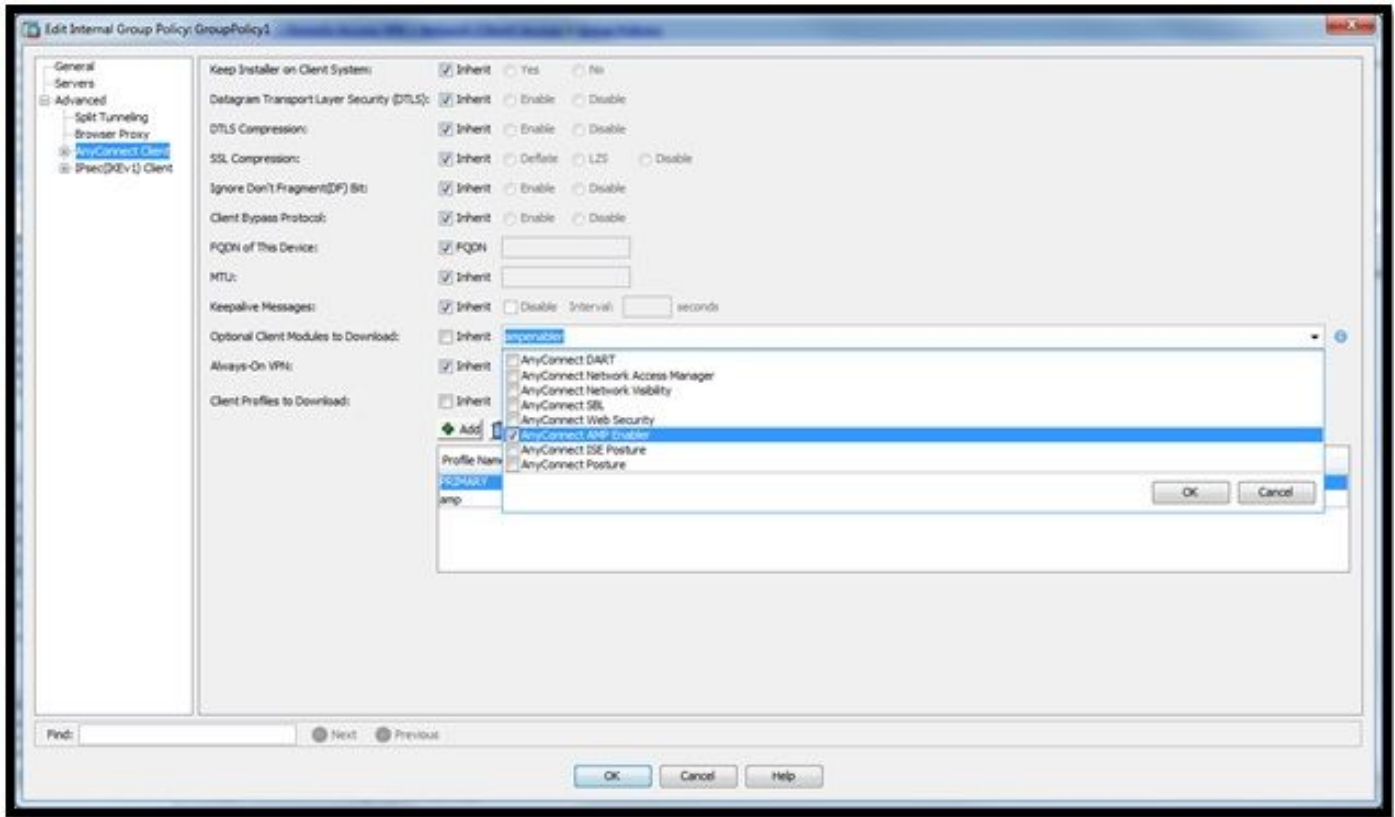
Profile Name	Profile Usage	Group Policy	Profile Location
PRIMARY	AnyConnect VPN Profile	GroupPolicy 1	disk0:/primary.xml
amp	AMP Enabler Service Profile	GroupPolicy 1	disk0:/amp.asp

Étape 2 : Éditez la stratégie de groupe pour télécharger l'Enabler d'AMPÈRE d'AnyConnect

- Naviguez vers la configuration > enlèvent le VPN d'accès > les stratégies de groupe >

éditent.

- Allez à **avancé > client d'AnyConnect > les modules facultatifs de client** aux télécharger.
- Choisissez l'**Enabler d'AMPÈRE d'AnyConnect**.



Étape 3 : Téléchargez la stratégie de FireAMP

Remarque: Avant que vous poursuiviez, déterminez si votre système répond aux exigences pour l'AMPÈRE du connecteur de Windows de points finaux.

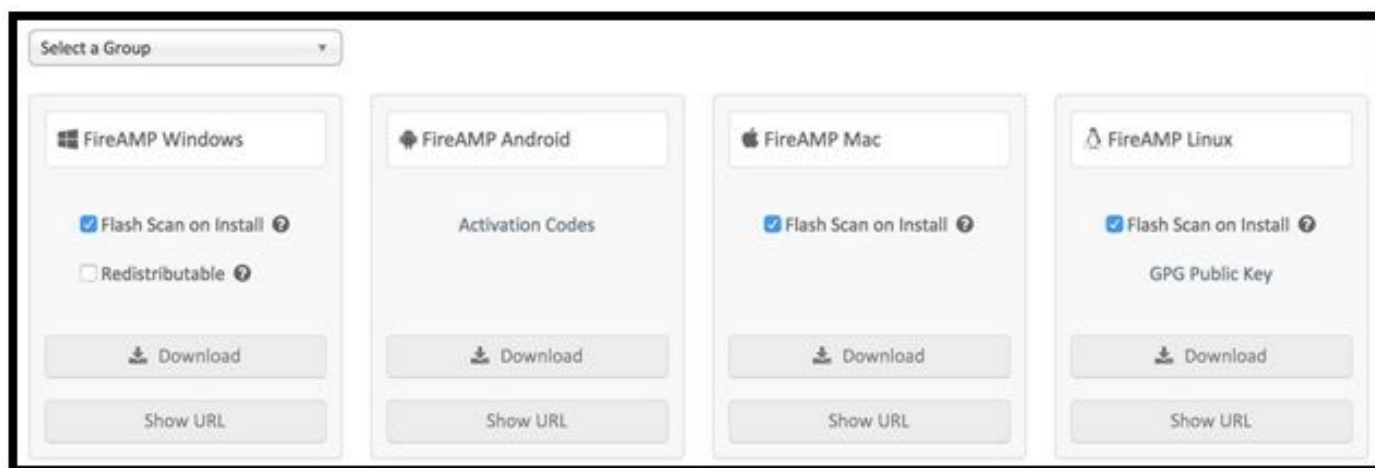
Configurations système requises pour l'AMPÈRE pour le connecteur de Windows de points finaux

Ce sont les configurations système minimales pour le connecteur de FireAMP basé sur le système d'exploitation Windows. Le connecteur de FireAMP prend en charge des versions de 32 bits et 64-bit de ces systèmes d'exploitation.

<u>Système d'exploitation</u>	Processeur	Mémoire	Espace disque, Mode de nuage seulement	Espace disque
Microsoft Windows XP avec Service Pack 3 ou plus tard	500 MHz ou processeur plus rapide	256MB RAM	L'espace disque dur disponible du Mo 150 - mode réservé au nuage	L'espace disque dur disponible 1GB - TÉTRA
Microsoft Windows Vista avec Service Pack 2 ou plus tard	1 gigahertz ou processeur plus rapide	RAM DU MO 512	L'espace disque dur disponible du Mo 150 - mode réservé au nuage	L'espace disque dur disponible 1GB - TÉTRA
Microsoft Windows 7	1 gigahertz ou processeur plus	1 RAM DE GO	L'espace disque dur disponible du	L'espace disque dur disponible

	rapide		Mo 150 - mode réservé au nuage	1GB - TÉTRA
Microsoft Windows 8 et 8.1 (exige le connecteur 3.1.4 de FireAMP ou plus tard)	1 gigahertz ou processeur plus rapide	RAM DU MO 512	L'espace disque dur disponible du Mo 150 - mode réservé au nuage	L'espace disque dur disponible 1GB - TÉTRA
Microsoft Windows Server 2003	1 gigahertz ou processeur plus rapide	RAM DU MO 512	L'espace disque dur disponible du Mo 150 - mode réservé au nuage	L'espace disque dur disponible 1GB - TÉTRA
Microsoft Windows Server 2008	2 gigahertz ou processeurs plus rapides	RAM DU GO 2	L'espace disque dur disponible du Mo 150 - Mode de nuage seulement	L'espace disque dur disponible 1GB - TÉTRA
Microsoft Windows Server 2012 (exige le connecteur 3.1.9 de FireAMP ou plus tard)	2 gigahertz ou processeurs plus rapides	RAM DU GO 2	L'espace disque dur disponible du Mo 150 - Mode de nuage seulement	Le 1 espace disque dur disponible de Go - TÉTRA

La page de connecteur de téléchargement te permet au téléchargement les modules d'installer pour chaque type de connecteur de FireAMP ou copie l'URL où ils peuvent être téléchargés. Ce module peut être placé sur une part du réseau ou être distribué par l'intermédiaire du logiciel de gestion. L'URL de téléchargement peut être envoyé aux utilisateurs afin de leur permettre pour le télécharger et installer eux-mêmes qui peut être téléchargé pour des utilisateurs distants.



Sélectionnez un groupe

- **Audit seulement** : Utilisé quand vous apprenez au sujet du produit et voulez toujours l'installer sans n'importe quelle incidence sur vos systèmes actuels.
- **Protégez** : Utilisé pendant le fonctionnement normal et vous voulez que FireAMP mette en quarantaine un fichier.
- **Sélection** : Utilisé quand vous avez un ordinateur infecté connu ou suspecté.
- **Serveur** : Utilisé quand vous installez un connecteur sur des Windows Server standard.
- **Contrôleur de domaine** : Utilisé quand vous installez un connecteur sur un contrôleur de

domaine windows.

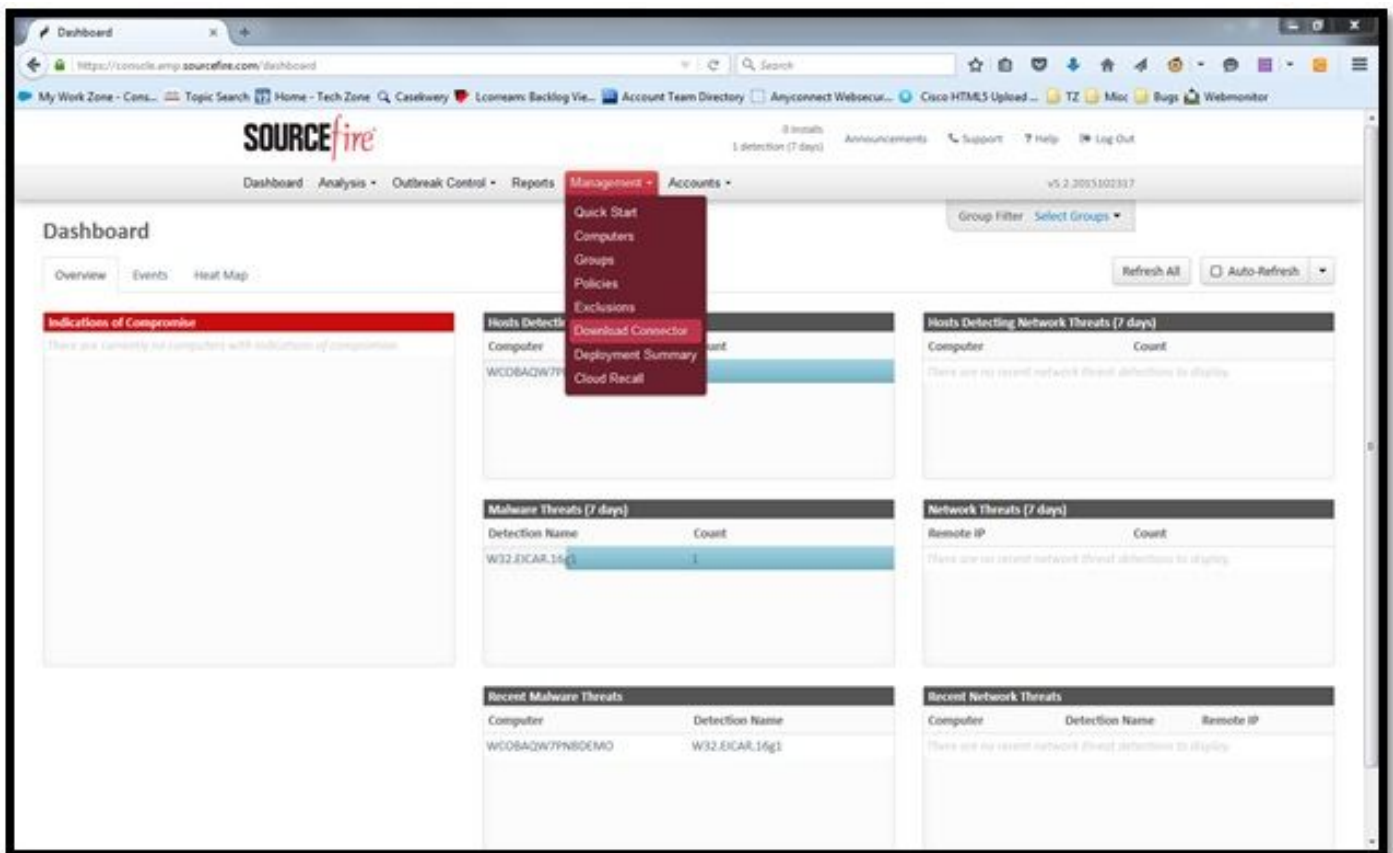
Caractéristiques

- **Le balayage instantané installé en fonction** : Passages de processus de balayage pendant l'installation. Ce balayage est basé sur nuage et exige une connexion réseau. Il est relativement rapide d'exécuter.
- **Redistribuable** : Cette option télécharge les installateurs de 32 bits et 64-bit en un module simple.

Remarque: Par défaut, il télécharge un petit fichier de bootstrapper (de ~500 KO) pour installer le connecteur de FireAMP. Cet exécutable détermine si les passages en machine des 32 ou un système d'exploitation et des téléchargements 64-bit et installe la version appropriée du connecteur de FireAMP.

Cependant, pour le VPN, vous devriez choisir de télécharger un installateur de redistribuable. C'est un fichier de Mo 30 qui contient les les deux 32 et installateurs 64-bit. Ce fichier peut être placé sur une part du réseau ou être poussé à tous les ordinateurs dans un groupe par l'intermédiaire d'un outil comme la Configuration Manager de System Center afin d'installer le connecteur de FireAMP sur de plusieurs ordinateurs. L'installateur également chacun des deux de bootstrapper et de redistribuable contiennent un fichier `policy.xml` qui est utilisé comme fichier de configuration pour l'installer.

Afin de télécharger le connecteur, naviguez vers le **connecteur de Gestion > de téléchargement**. Choisissez alors le type, et le **téléchargement** FireAMP (Windows, Android, MAC, Linux).



Dans ce cas, l'option d'audit pour le **connecteur de téléchargement** et l'installation pour l'ordinateur Windows ont été choisies.

Download Connector

Audit

FireAMP Windows

Flash Scan on Install ?

Redistributable ?

Download

Show URL

FireAMP Android

Activation Codes

Download

Show URL

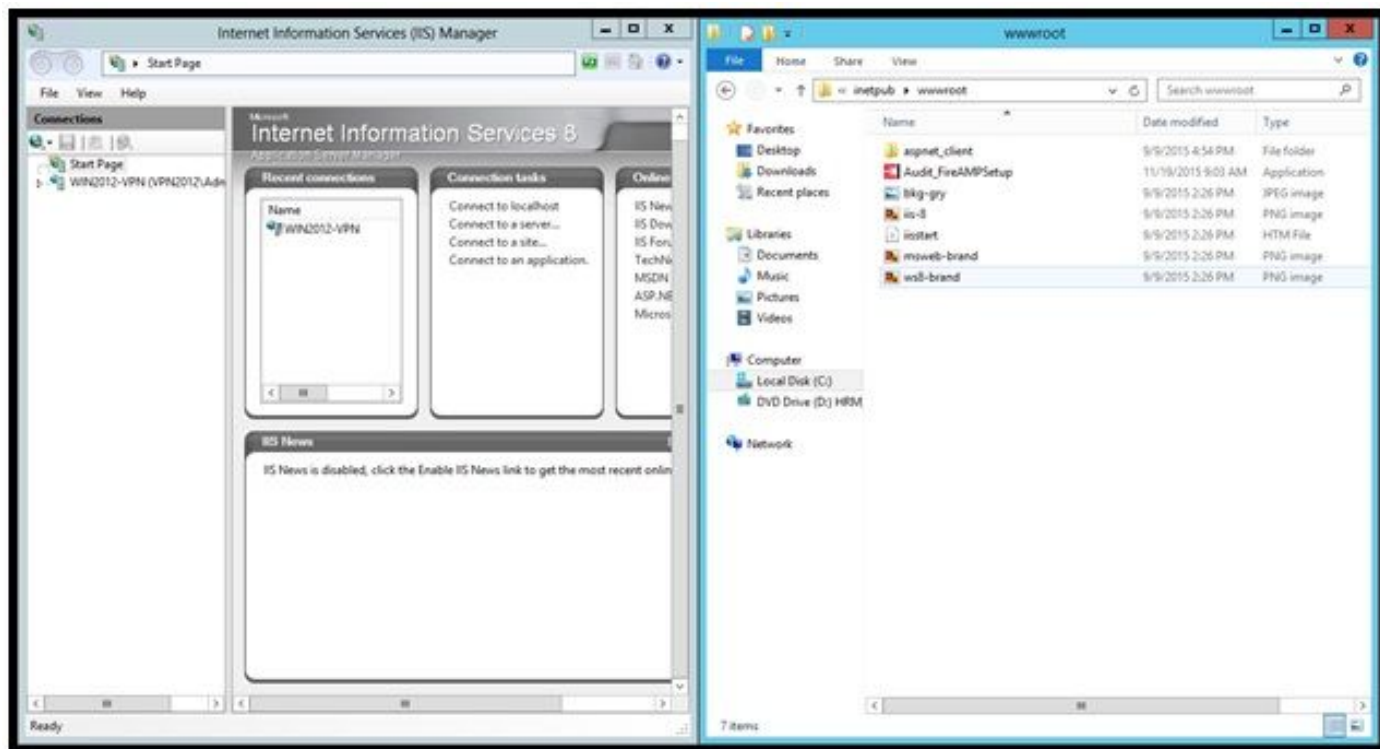
FireAMP Mac

Flash Scan on Install ?

Download

Show URL

Remarque: Quand ce fichier est téléchargé il génère un fichier .exe appelé, dans ce cas, Audit_FireAMPSetup.exe. Ce fichier a été envoyé au web server afin d'être disponible et téléchargé de l'ASA une fois que l'utilisateur demande la configuration pour l'AMPÈRE.

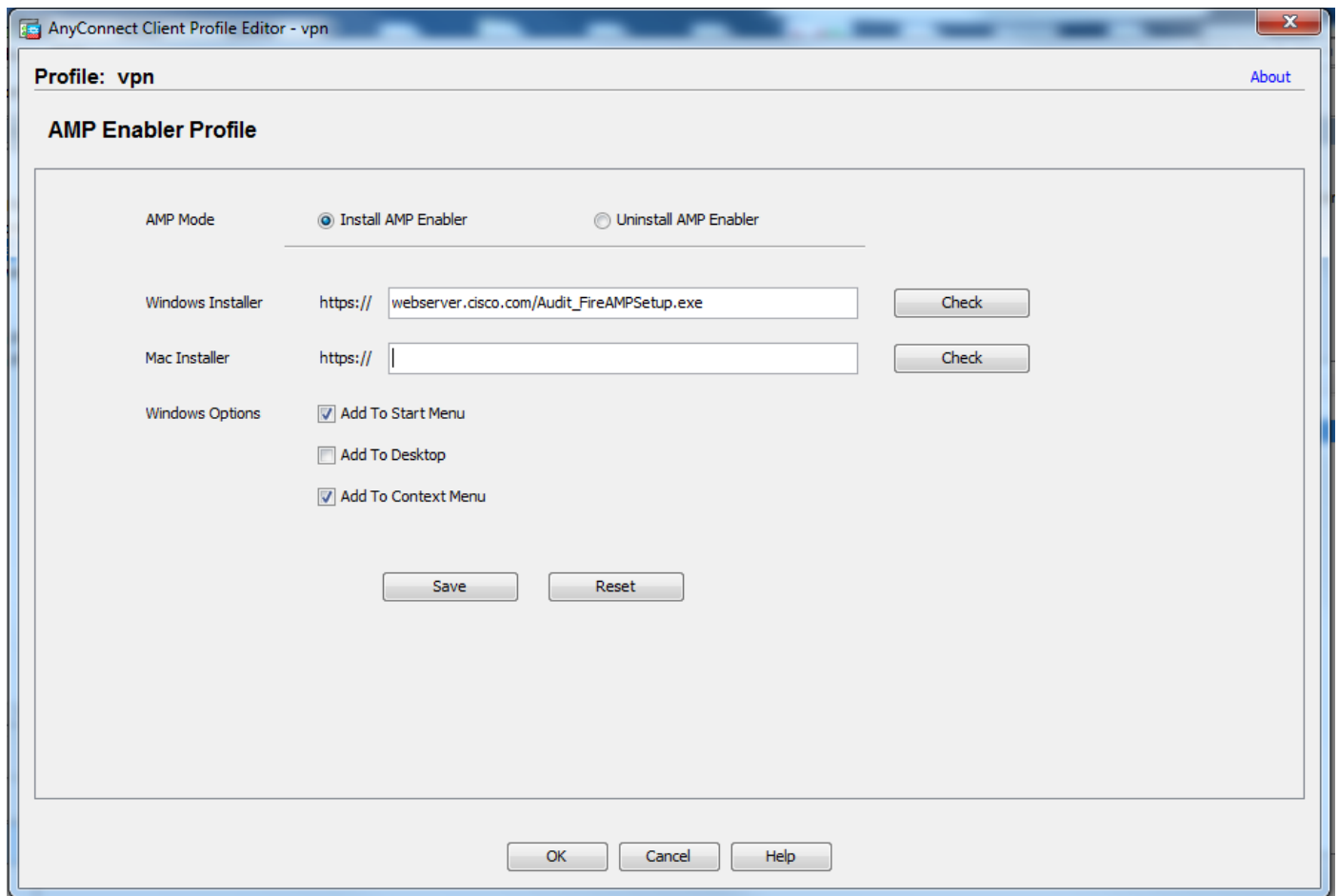


Étape 4 : Téléchargez le profil de client de sécurité Web

Retournez au profil d'AMPÈRE créé avant sur l'ASA (étape 1) et éditez le profil d'Enabler d'AMPÈRE :

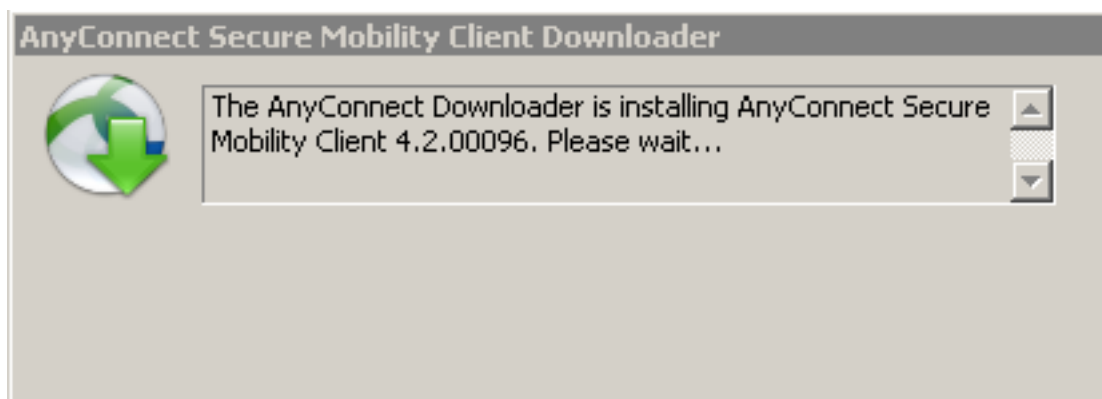
1. Pour le **mode d'AMPÈRE**, cliquez sur la case d'option d'**Enabler d'AMPÈRE d'installer**.
2. Dans le domaine d'**installer windows**, ajoutez l'IP pour le web server et le fichier pour le FireAMP.
3. **Les options de Windows** sont facultatives.

Cliquez sur OK et appliquez les modifications.



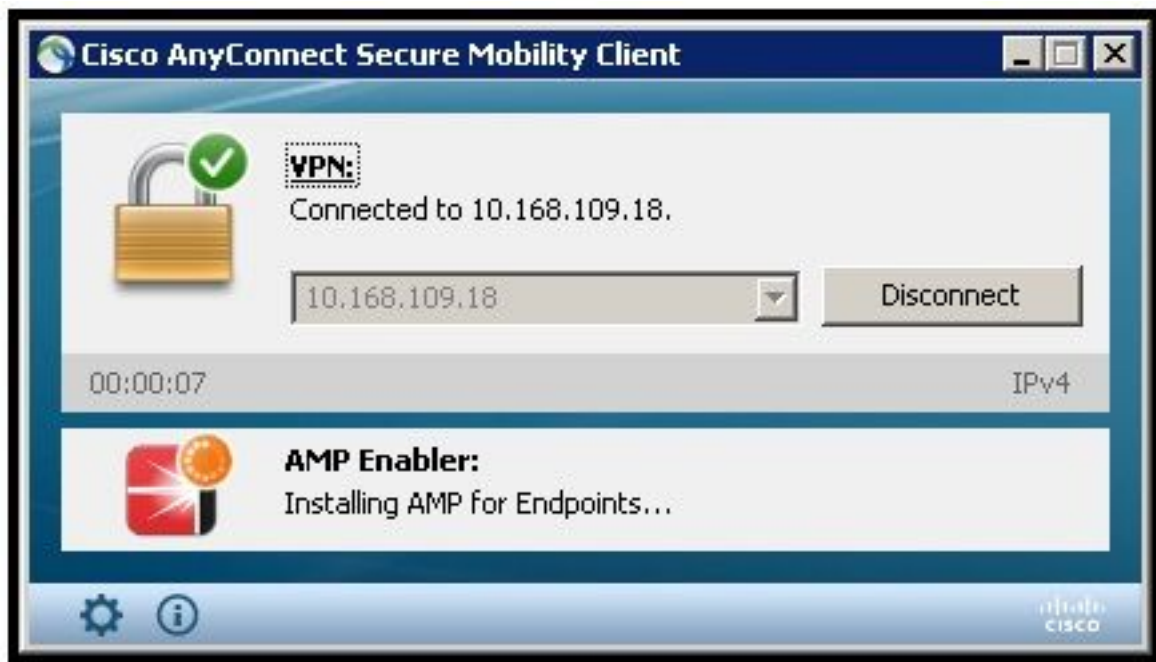
Étape 5 : Connectez à AnyConnect et vérifiez l'installation du module

Quand les utilisateurs d'Anyconnect VPN se connectent, l'ASA pousse le module d'Enabler d'AMPÈRE d'AnyConnect par le VPN. Pour les utilisateurs déjà ouverts une session, il est recommandé pour se fermer une session et ouvrir une session alors de retour pour que la fonctionnalité soit activée.



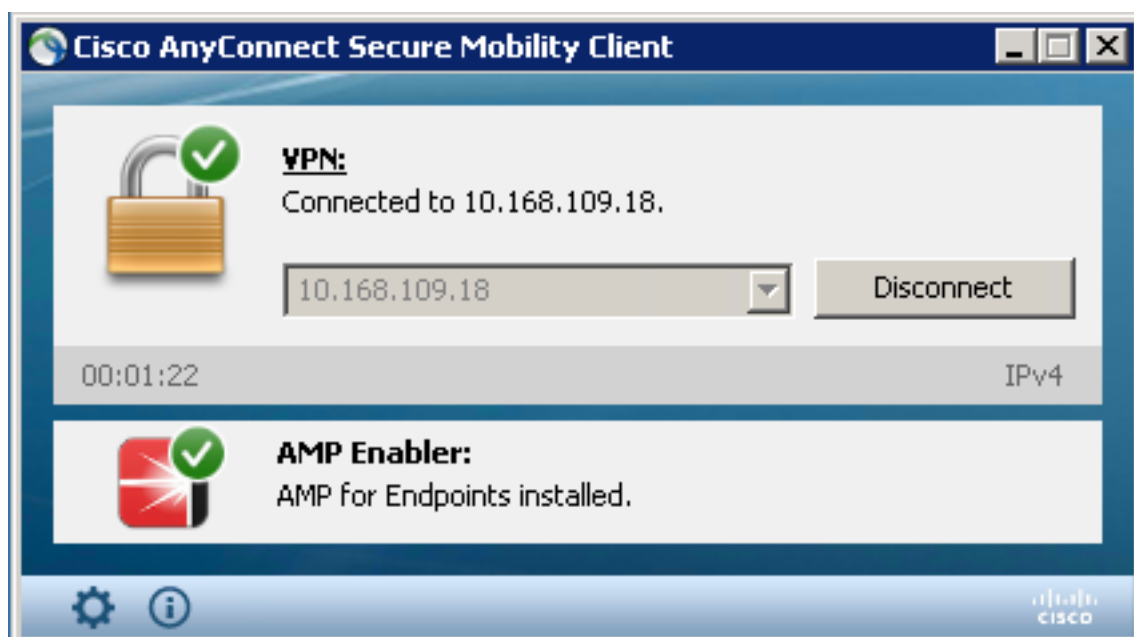
Étape 6 : Vérifiez la connexion VPN et l'Enabler d'AMPÈRE

Vérifiez si le VPN est connecté et l'Enabler d'AMPÈRE collecte la configuration du web server.



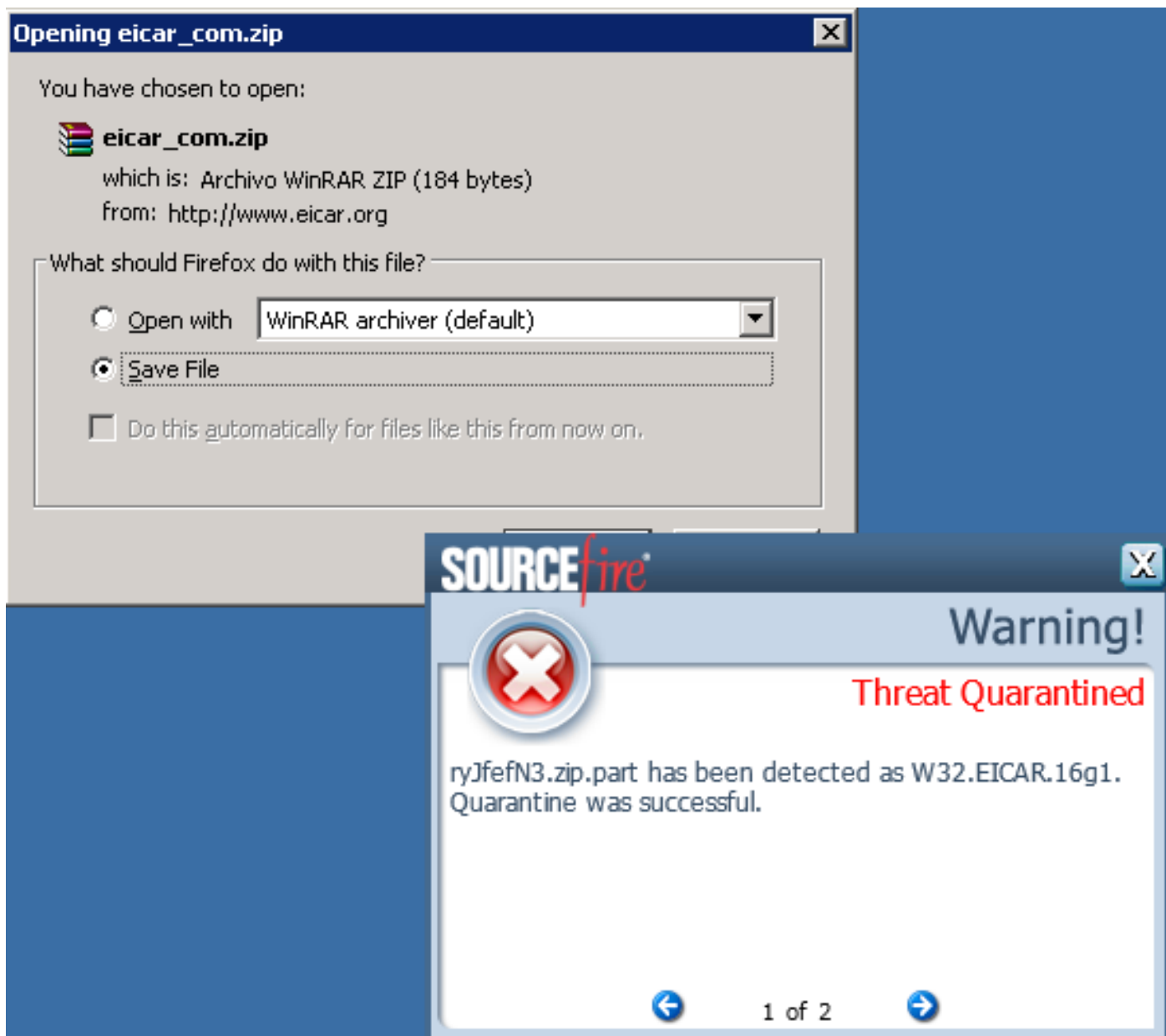
Étape 7 : Vérifiez AnyConnect et le vérifiez si tout est installé

Une fois que le VPN est connecté et la configuration du web server est installée, vérifiez AnyConnect et vérifiez tout est installé correctement.



Étape 8 : Test avec une chaîne d'Eicar contenue dans un fichier zip dans un ordinateur

Test avec une chaîne d'Eicar contenue dans un fichier zip dans un ordinateur afin de vérifier si tout fonctionne comme prévu.



Étape 9 : Résumé de déploiement

Cette page vous affiche qu'une liste de réussi et connecteur défectueux de FireAMP installe aussi bien que ceux en cours. Vous pouvez aller au [résumé de Gestion > de déploiement](#).

SOURCEfire 0 installs 1 detection (7 days) Announcements Support Help Log Out

Dashboard Analysis Outbreak Control Reports Management Accounts v5.2.2015102317

Deployment Summary Group Filter Select Groups

Show All Successful Installing Failed Deployments

✓ 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 Export to CSV

Étape 10 : Vérification de détection de thread

Cette page t'affiche une liste de thread bloqués par le connecteur de FireAMP et également les ordinateurs affectés. Vous pouvez aller au **tableau de bord**.

SOURCEfire 1 install 8 detections (7 days) Announcements Support Help Log Out

Dashboard Analysis Outbreak Control Reports Management Accounts v5.2.2015102317

Dashboard Group Filter Protect Refresh All Auto-Refresh

Overview Events Heat Map

Indications of Compromise
WCOBAQW7PNBDEMO Mark Resolved
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
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.		

Informations supplémentaires

Le logiciel incompatible pour le connecteur de FireAMP Windows sont :

- Alarme de zone par Check Point
- Noir de carbone
- Logiciel AppGuard recherche

Informations connexes

- [Configurez l'Enabler d'AMPÈRE](#)
- [Support et documentation techniques - Cisco Systems](#)