AnyConnect 4.x および AMP イネーブラを介した AMP モジュールのインストールと設定

目次

概要

この資料は AnyConnect でエンドユーザ システムで Advanced Malware Protection （ AMP ）モジュールをインストールし、設定するために方式を記述したものです。

メディアとして AnyConnect AMP イネーブラーがエンドポイントのための AMP を展開するのに使用されています。 これにより、社内でローカルにホストされているサーバからエンドポイントのサブセットにエンドポイント向け AMP ソフトウェアがプッシュされ、AMP サービスが既存のユーザ ベースにインストールされます。 このアプローチはネットワークで起こる潜在的な malware 脅威を、取除きそれらの脅威を、侵害から保護する企業を検出する 追加 の セキュリティ エージェントを AnyConnect ユーザベース 管理者に与えます。 これにより、ダウンロードにかかる時間と帯域幅が節約され、ポータル側で変更を行う必要がありません。また、この作業を行う際に、エンドポイントに認証クレデンシャルが送信されません。

前提条件

要件

- AnyConnect セキュア モビリティ クライアント バージョン 4.x
- FireAMP / エンドポイント向け AMP
- AnyConnect Plus / Apex ライセンス

- Adaptive Security Device Manager （ASDM）バージョン 7.3.2 または それ 以降

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- 適応型セキュリティ アプライアンス（ASA）ソフトウェア（ASA）ソフトウェア バージョン 9.5.1 との 5525
- Microsoft Windows 7 専門 64 ビットの AnyConnect セキュア モビリティ クライアント 4.2.00096
- ASDM バージョン 7.5.1(112)

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

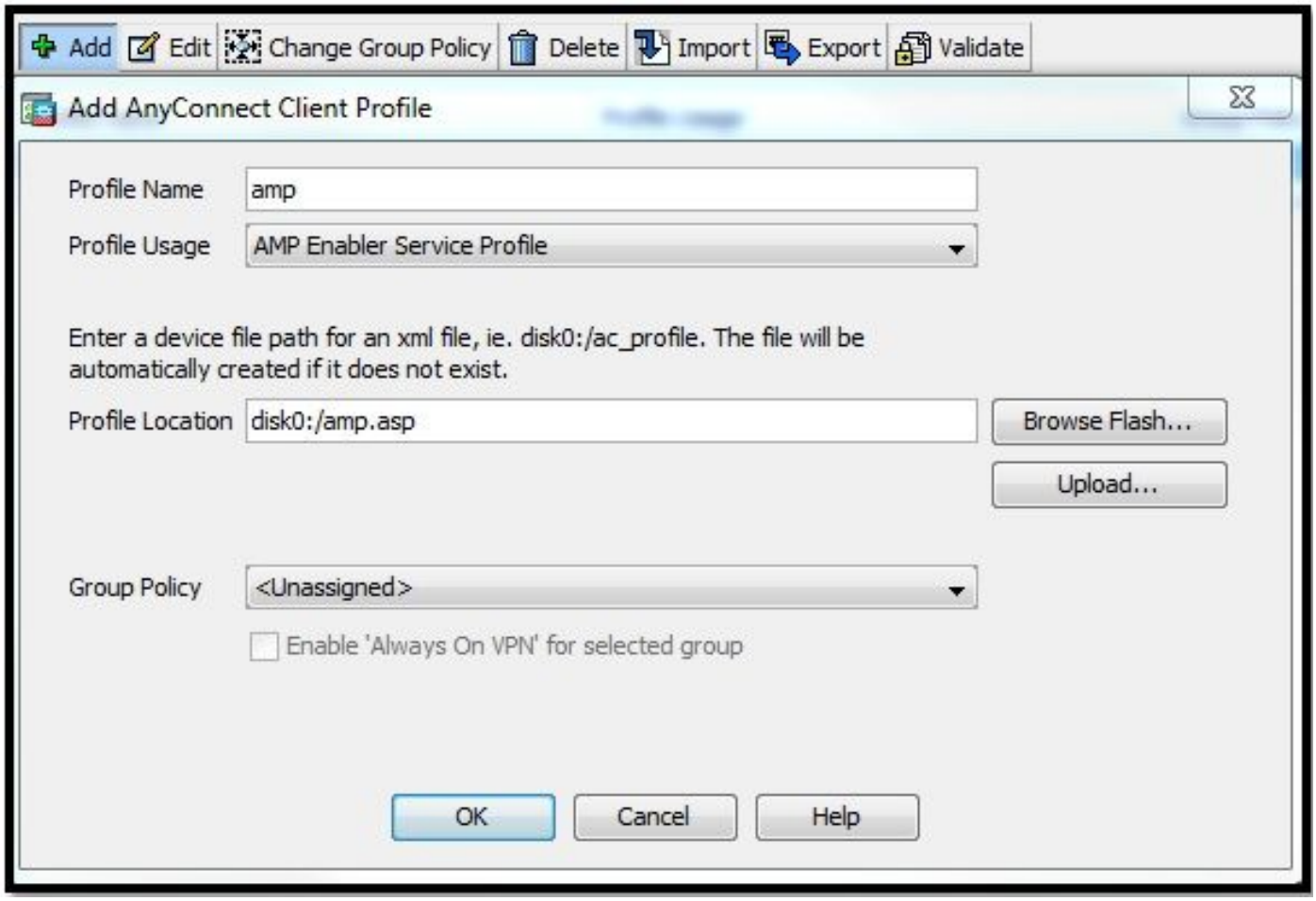
ASA を介した AMP イネーブラのための AnyConnect の導入

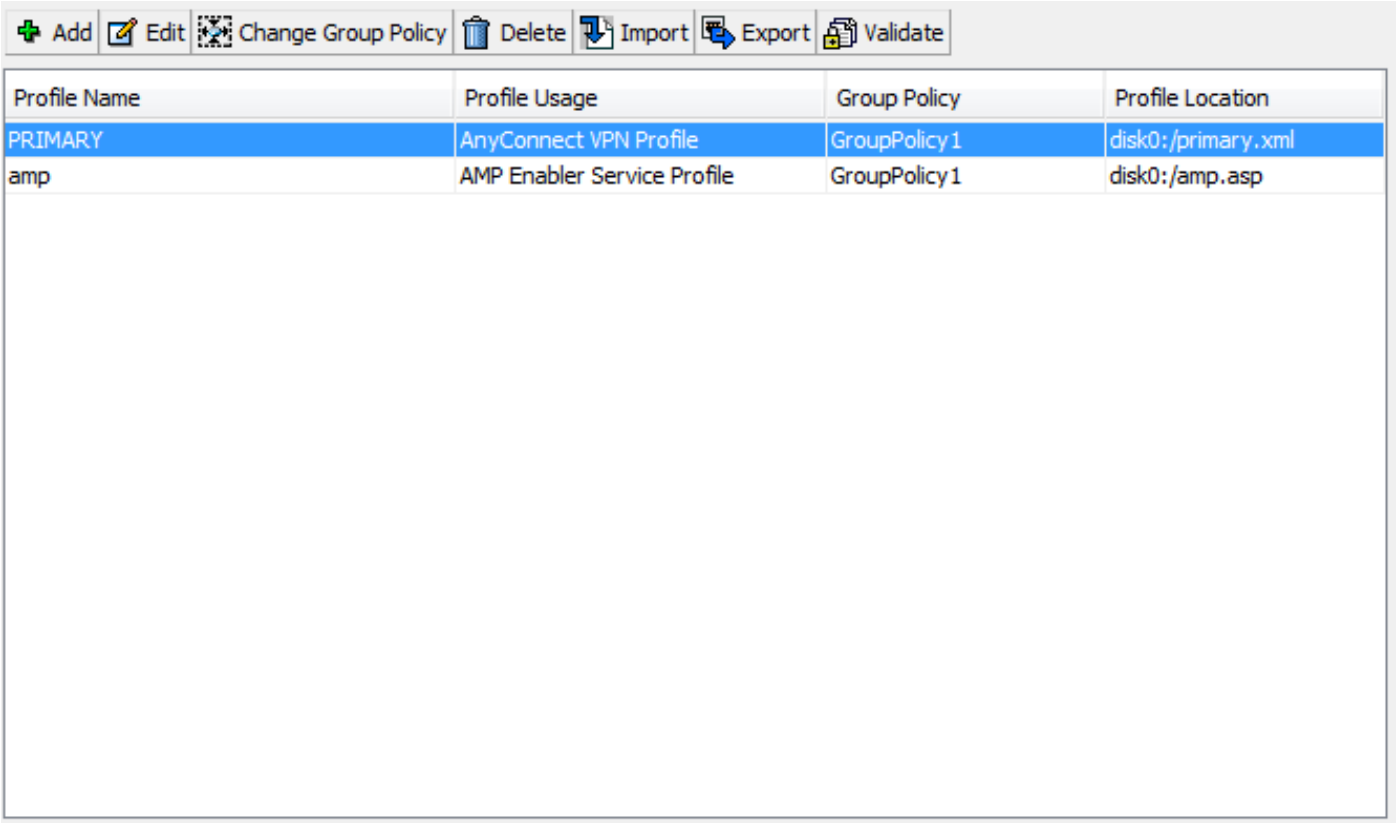
設定の手順は次の通りです:

- AnyConnect AMP イネーブラー クライアント プロファイルを設定して下さい。
- AnyConnect VPNグループ ポリシーを編集し、AMP イネーブラー サービス プロファイルをダウンロードして下さい。
- Webサーバから設定を得るために AMP プロファイルを編集して下さい。
- ユーザ マシンでインストールを検証します。

ステップ 1： AnyConnect AMP イネーブラー クライアント プロファイルを設定して下さい

- **設定 > リモートアクセス VPN > ネットワーク（クライアント）アクセス > AnyConnect クライアント プロファイル**へのナビゲート。
- **AMP イネーブラー サービス プロファイルを**追加して下さい。

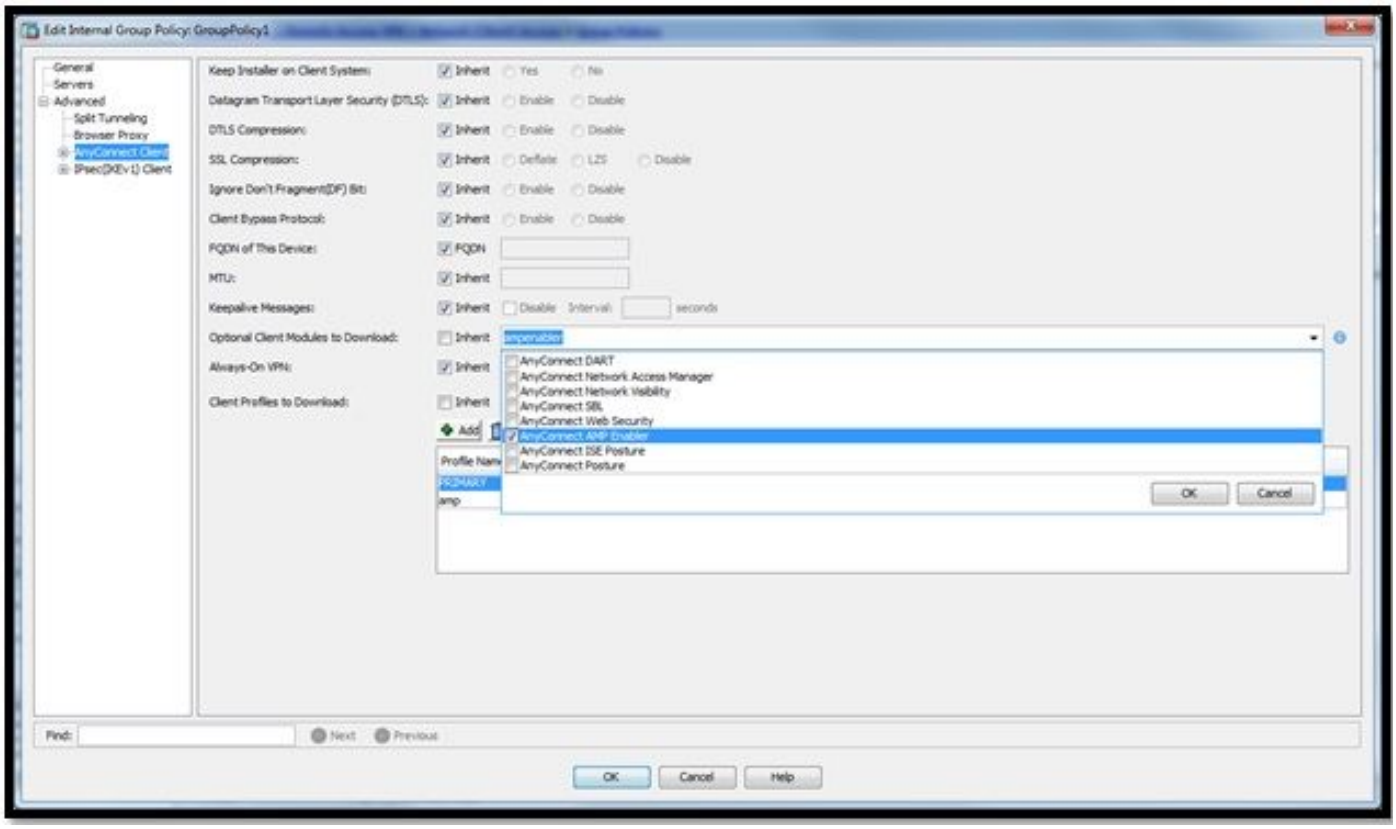




ステップ 2： AnyConnect AMP イネーブラをダウンロードするためのグループ ポリシーの編集

- [Configuration] > [Remove Access VPN] > [Group Policies] > [Edit] の順に移動します。

- > AnyConnect クライアントは高度に > ダウンロードするべきオプションのクライアント モジュール行きます。
- AnyConnect AMP イネーブラーを選択して下さい。



手順 3： FireAMP ポリシーのダウンロード

注: 続行する前に、システムがエンドポイント Windows コネクタの AMP のための必要条件を満たしたかどうか確認して下さい。

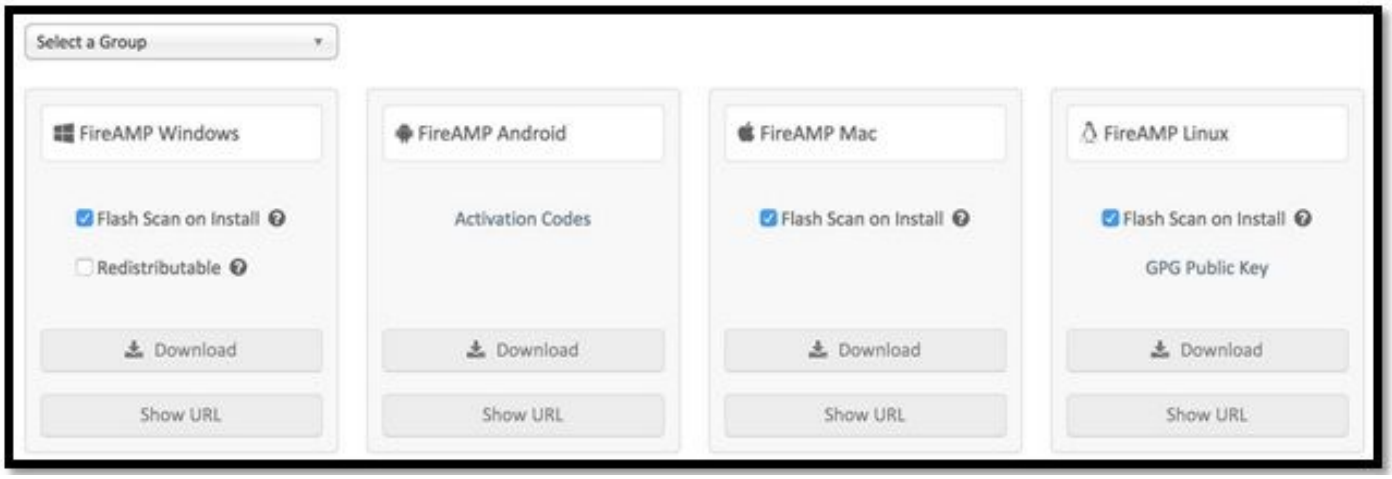
AMP for Endpoints Windows Connector のシステム要件

これらはウィンドウズオペレーティングシステムに基づいて FireAMP コネクタ用の最小システム要件です。 FireAMP Connector は、次のオペレーティング システムの 32 ビット バージョンと 64 ビット バージョンをサポートします。

オペレーティング システム	プロセッサ	「メモリ	ディスク領域、クラウド専用モード	ディスク領域
Microsoft Windows XP (Service Pack 3 以降)	500 MHz 以上のプロセッサ	メモリ 256 MB	150 MB の使用可能なハード ディスク領域 - クラウド専用モード	1 GB の使用可能なハード ディスク領域 - TETRA
Microsoft Windows Vista (Service Pack 2 以降)	1 GHz 以上のプロセッサ	メモリ 512 MB	150 MB の使用可能なハード ディスク領域 - クラウド専用モード	1 GB の使用可能なハード ディスク領域 - TETRA
Microsoft Windows 7	1 GHz 以上のプロセッサ	メモリ 1 GB	150 MB の使用可能なハード ディスク領域 - クラウド専用モード	1 GB の使用可能なハード ディスク領域 - TETRA

Microsoft Windows 8 および 8.1 (FireAMP Connector 3.1.4 以降が必要)	1 GHz 以上のプロセッサ	メモリ 512 MB	150 MB の使用可能なハード ディスク領域 - クラウド専用モード	1 GB の使用可能なハード ディスク領域 - TETRA
Microsoft Windows Server 2003	1 GHz 以上のプロセッサ	メモリ 512 MB	150 MB の使用可能なハード ディスク領域 - クラウド専用モード	1 GB の使用可能なハード ディスク領域 - TETRA
Microsoft Windows Server 2008	2 GHz 以上のプロセッサ	メモリ 2 GB	150 MB の使用可能なハード ディスク領域 - クラウド専用モード	1 GB の使用可能なハード ディスク領域 - TETRA
Microsoft Windows Server 2012 (FireAMP Connector 3.1.9 以降が必要)	2 GHz 以上のプロセッサ	メモリ 2 GB	150 MB の使用可能なハード ディスク領域 - クラウド専用モード	1 GB の使用可能なハード ディスク領域 - TETRA

ダウンロード コネクタ ページはダウンロードに FireAMP コネクタの各型のためのインストール パッケージを与えるか、またはダウンロードすることができる URL をコピーします。 このパッケージはネットワーク共有に置かれるか、または管理用ソフトによって配ることができます。 ダウンロード URL はユーザにそれらを自身リモートユーザ向けにダウンロードすることができるそれをダウンロードし、インストールすることを許可するために E-メールを送ることができます。



[Select a Group]

- **[Audit Only]**： まだ製品について学習中であり、既存のシステムに影響を与えずにインストールする場合に使用します。
- **[Protect]**： 通常の操作中に、FireAMP でファイルの検疫を行う場合に使用します。
- **[Triage]**： 感染が確認されたマシンまたは感染が疑われるマシンがある場合に使用します。
- **[Server]**： 標準的 な ウィンドウズ サーバでコネクタをインストールする時使用される。
- **[Domain Controller]**： Windows ドメインコントローラでコネクタをインストールする時使用される。

機能

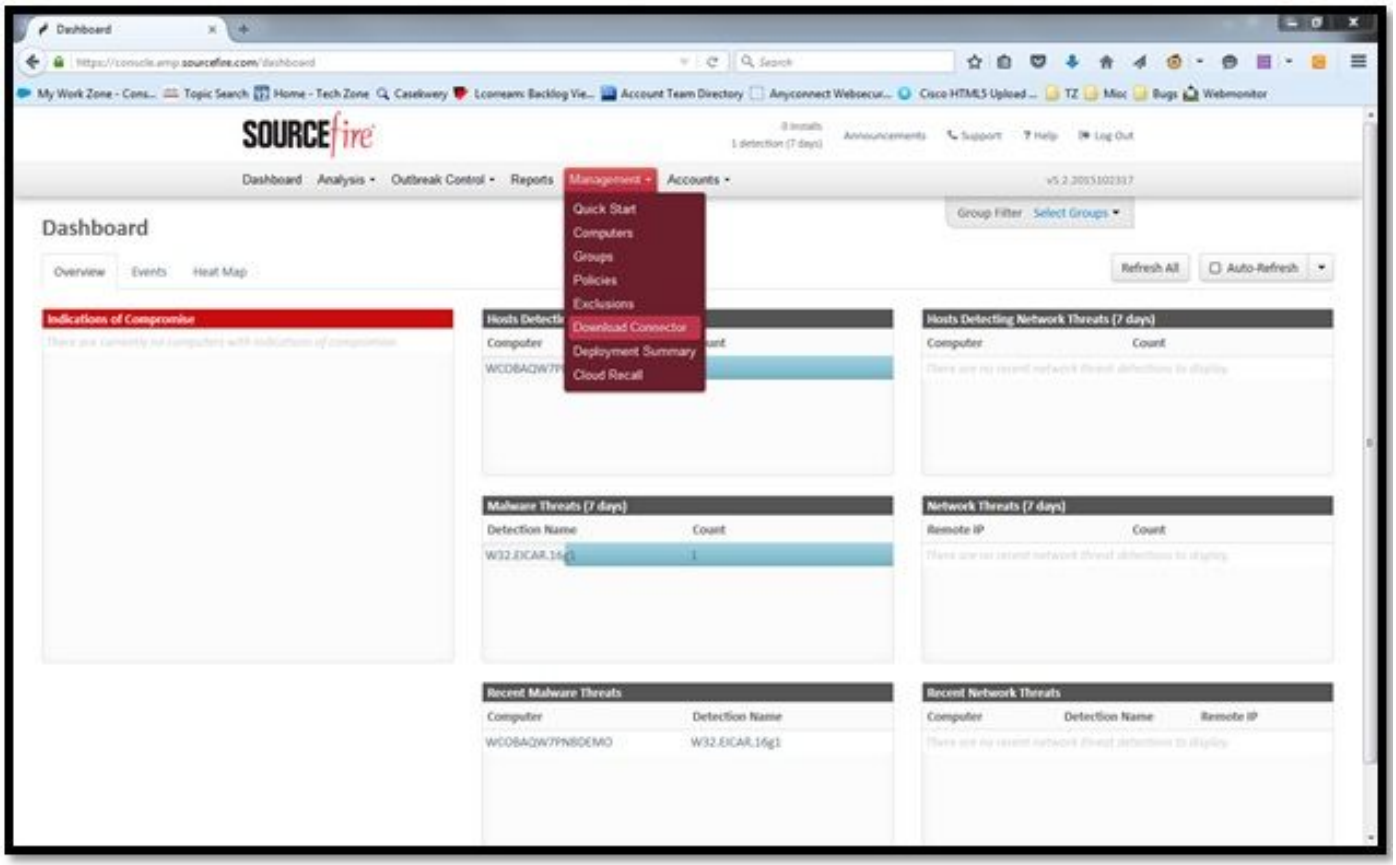
- **[Flash Scan on Install]**： インストールの間のスキャン プロセス実行。 このスキャンはクラウド ベースで、ネットワーク接続を必要とします。 それは実行することは比較的に高速です。
- **[Redistributable]**： このオプションでは、32 ビット インストーラと 64 ビット インストーラ

が 1 つのパッケージでダウンロードされます。

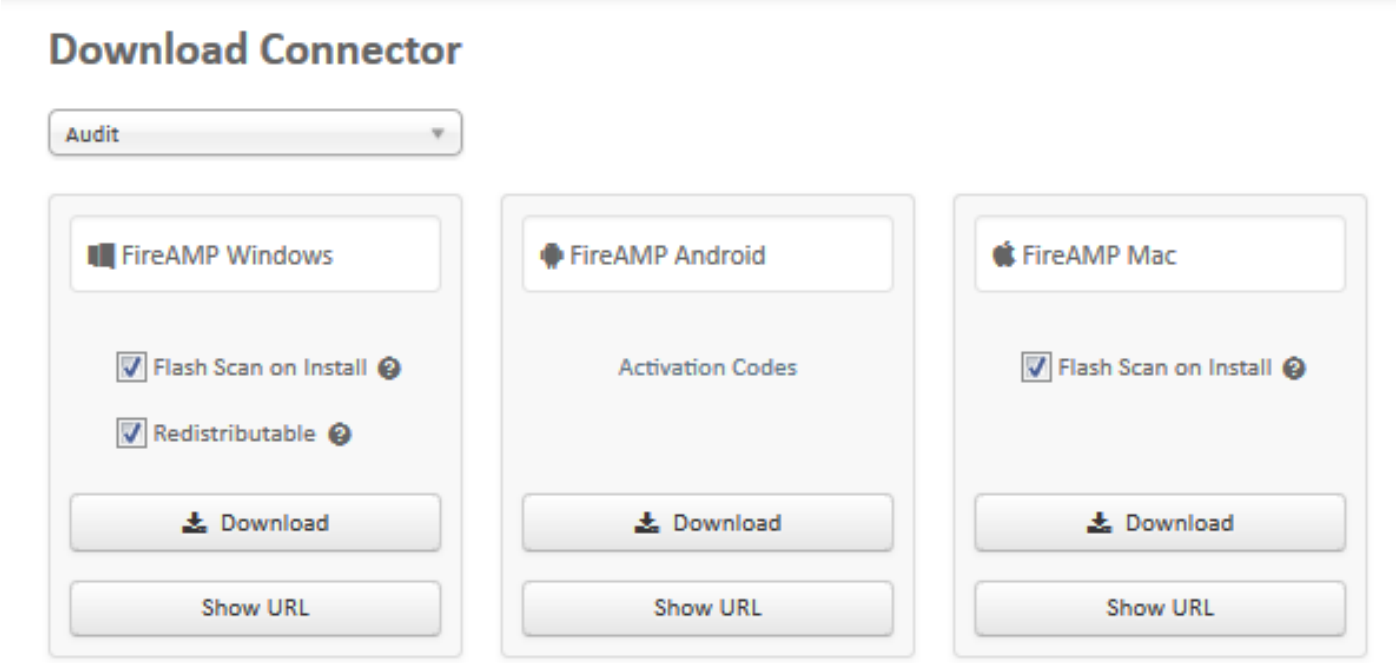
注: デフォルトで、それは FireAMP コネクタをインストールするために小さい (~500 KB) ブートストラップ ファイルをダウンロードします。 この実行可能モジュールはコンピュータが 32 または 64 ビット オペレーティング システムを実行した確認し、FireAMP コネクタの適切なバージョンをかどうかダウンロードし、インストールします。

ただし、VPN のために、redistributable インストーラをダウンロードすることを選択するべきです意図します。 これは、32 ビット インストーラと 64 ビット インストーラの両方を含む 30 MB のファイルです。 FireAMP Connector を複数のコンピュータにインストールするために、このファイルをネットワーク共有に配置することも、System Center Configuration Manager などのツールを介してグループ内のすべてのコンピュータにプッシュすることもできます。 ブートストラッパと再配布可能インストーラの両方に、インストール用のコンフィギュレーション ファイルとして使用される policy.xml ファイルも含まれています。

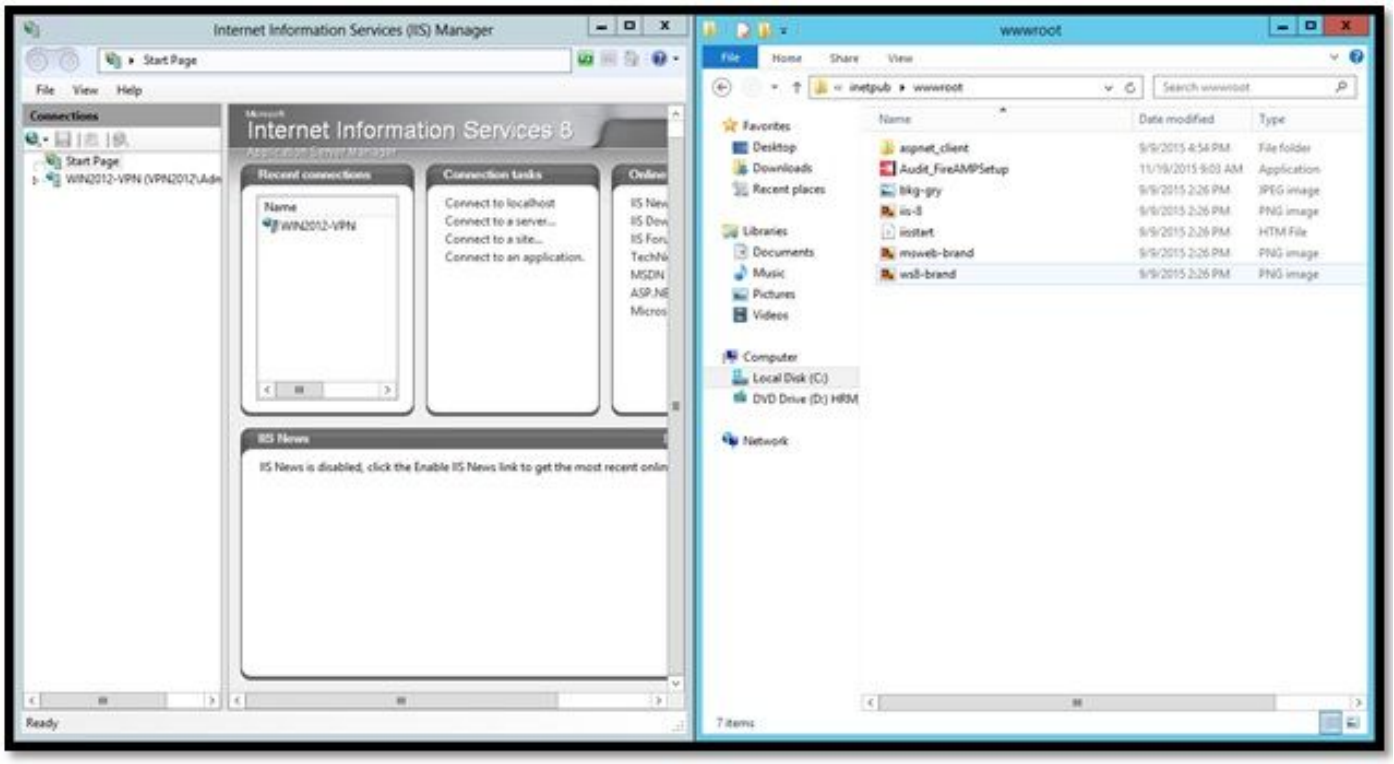
コネクタを、ナビゲート **管理 > ダウンロード コネクタ**にダウンロードするため。 それから『 Type』 を選択 し、FireAMP （ Windows、Android、Mac、Linux ）を**ダウンロードして下さい**。



この場合、**ダウンロード コネクタ**用の**監査** オプションおよび Windows マシンのためのインストールは選択されました。



注: このファイルがダウンロードされるとき、この場合呼出される、`.exe` ファイルを `Audit_FireAMPSetup.exe` 生成します ファイルは Webサーバに利用可能 ユーザが AMP の設定を頼めばであるために送信 され、ASA からダウンロードされました。

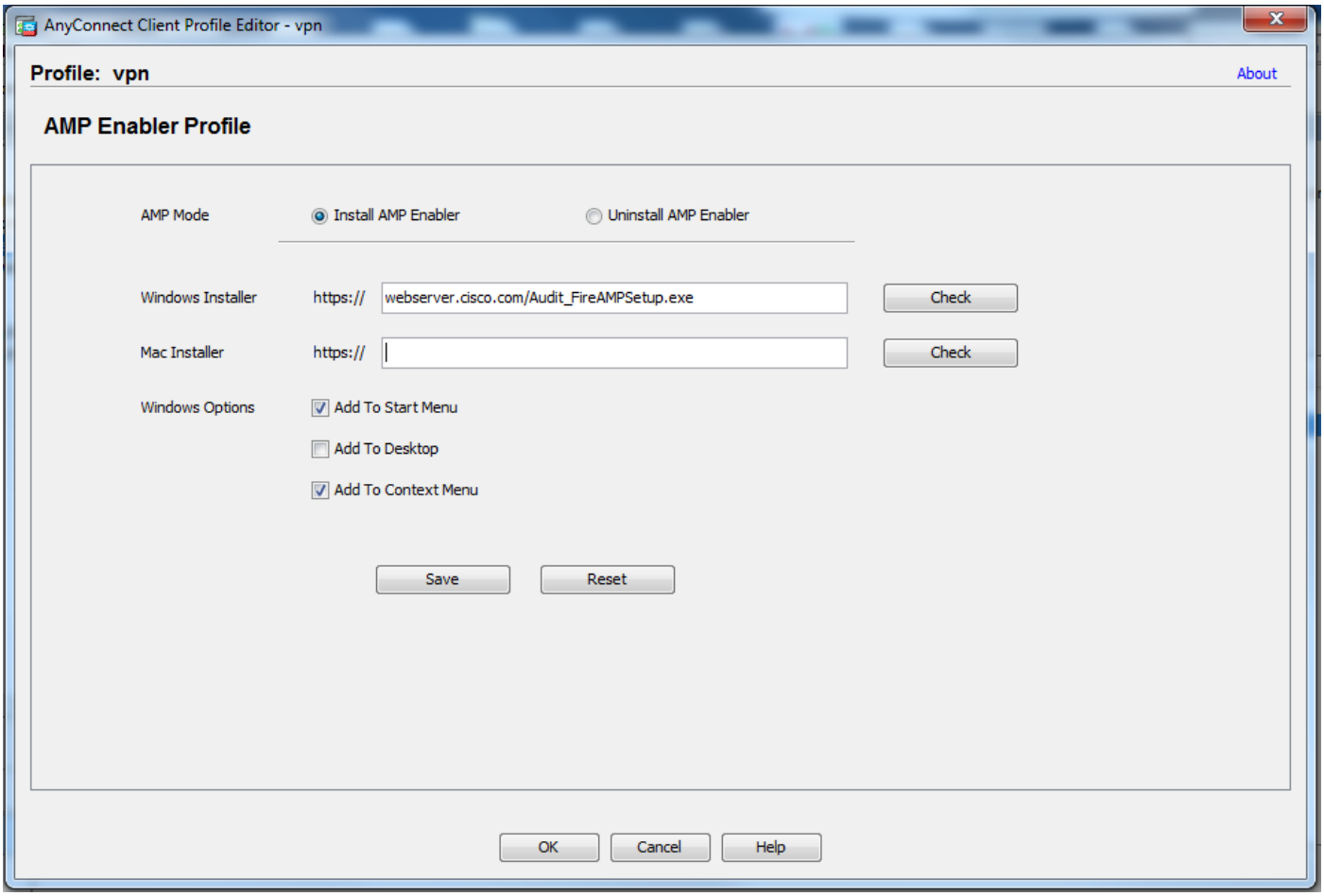


ステップ 4： Web セキュリティ クライアント プロファイルをダウンロードして下さい

ASA で前に作成される AMP プロファイルに戻って下さい（1）ステップは **AMP イネーブラー プロファイルを**編集し、：

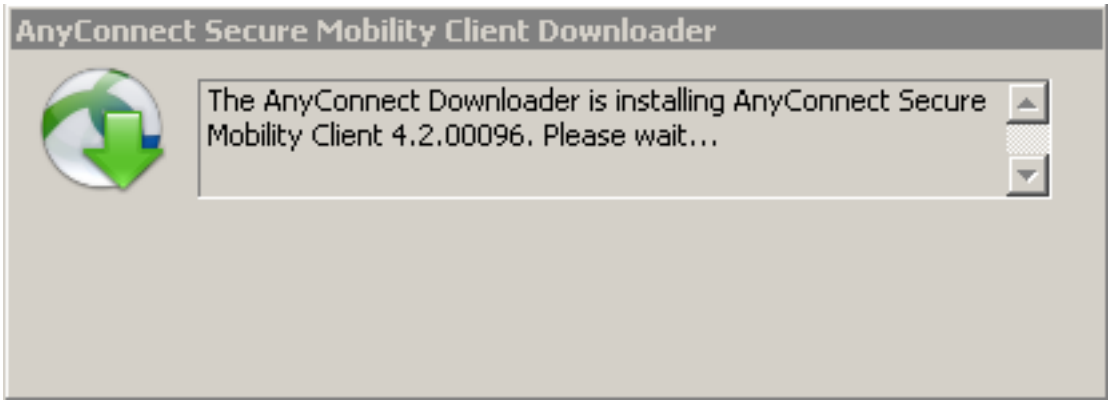
1. **AMP モード**に関しては、**インストール AMP イネーブラー** オプション ボタンをクリックして下さい。
2. **Windows インストーラ** フィールドでは、Webサーバのための IP および FireAMP のためのファイルを追加して下さい。
3. [Windows Options] はオプションです。

[OK] をクリックし、変更を適用します。



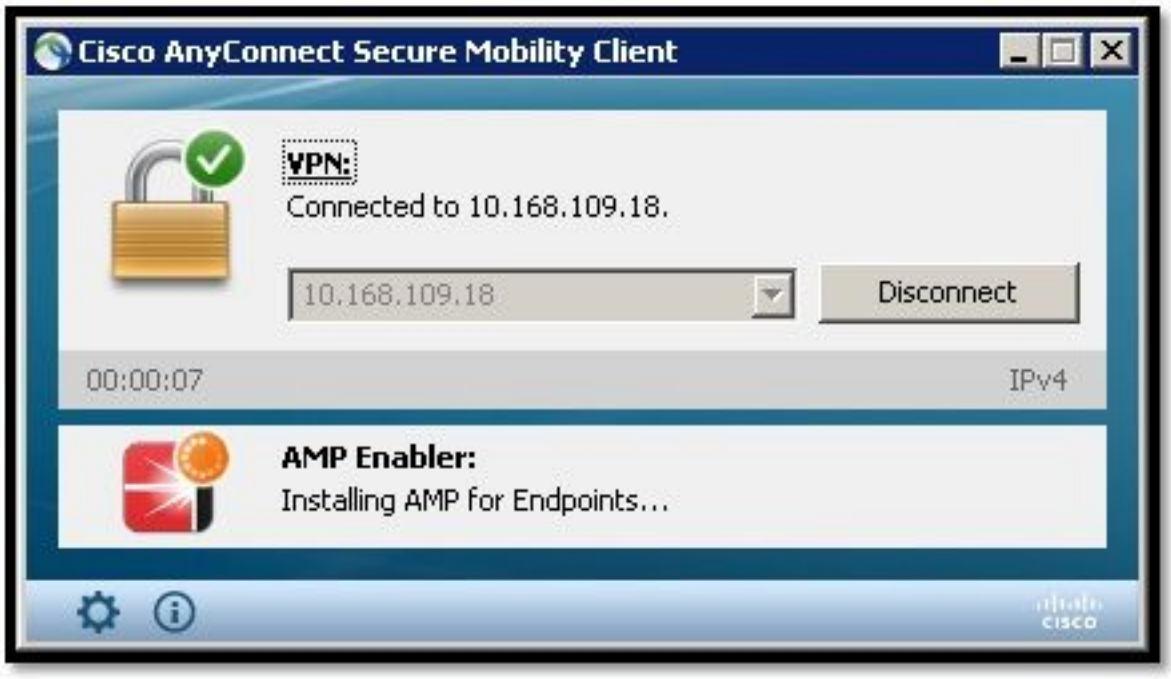
ステップ 5： AnyConnect への接続とモジュールのインストールの検証

Anyconnect VPN ユーザが接続するとき、ASA は VPN に AnyConnect AMP イネーブラー モジュールを押通します。 既にログイン ユーザ向けに、ログオフし、次に機能性のためのログイン背部有効に なることを推奨します。



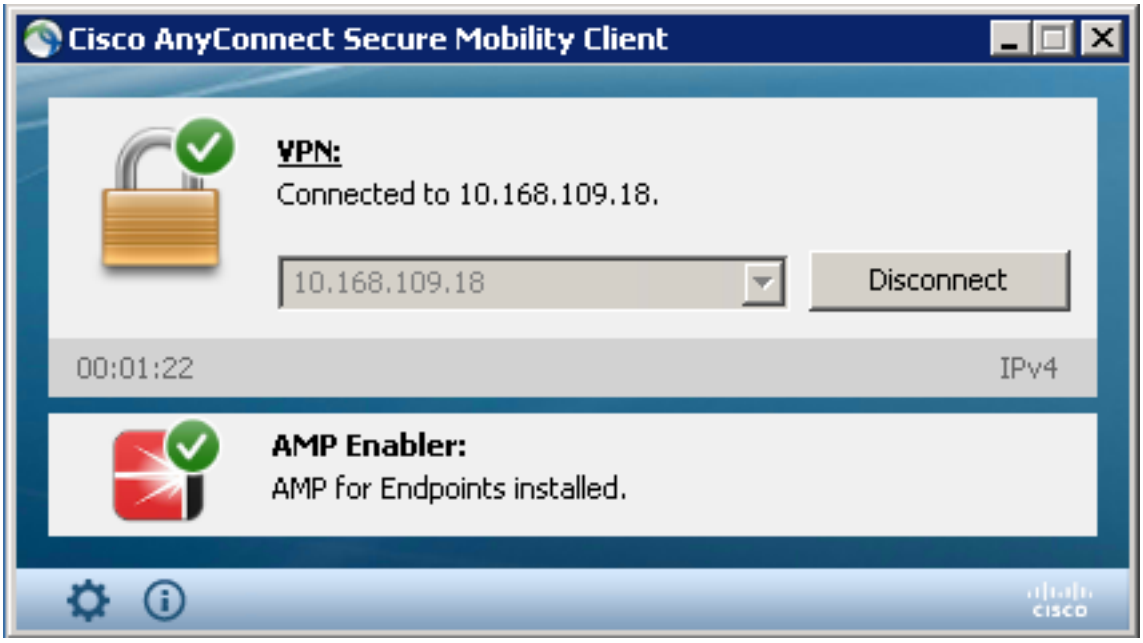
ステップ 6： VPN 接続および AMP イネーブラの検証

VPN が接続されており、**AMP イネーブラ**が Web サーバから設定を収集するかどうかを検証します。



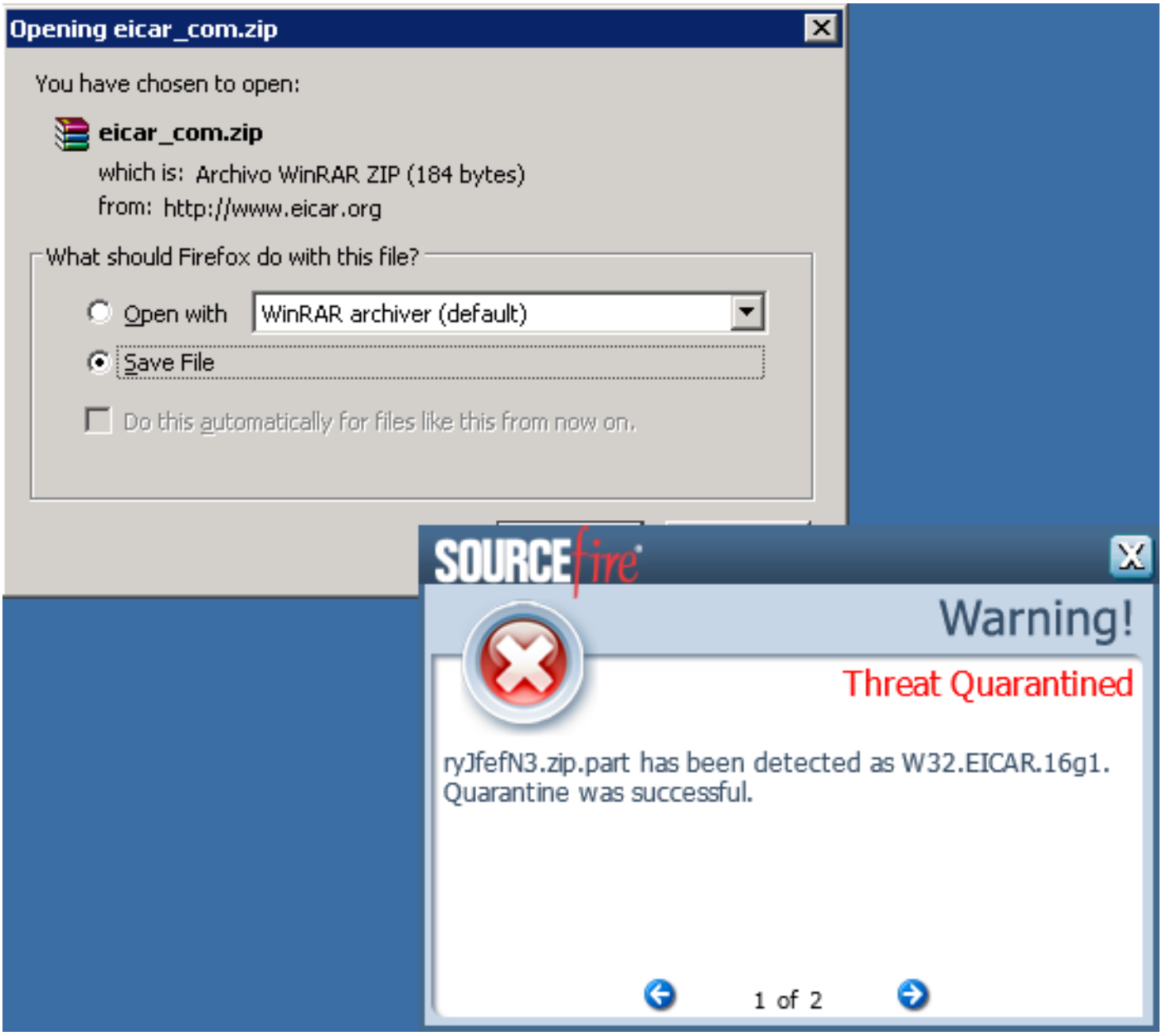
ステップ 7：AnyConnect の確認とすべてのコンポーネントがインストールされているかどうかの検証

VPN が接続され、Webサーバの設定がインストールされていたら、AnyConnect をチェックし、すべてがきちんとインストールされていることを確認して下さい。



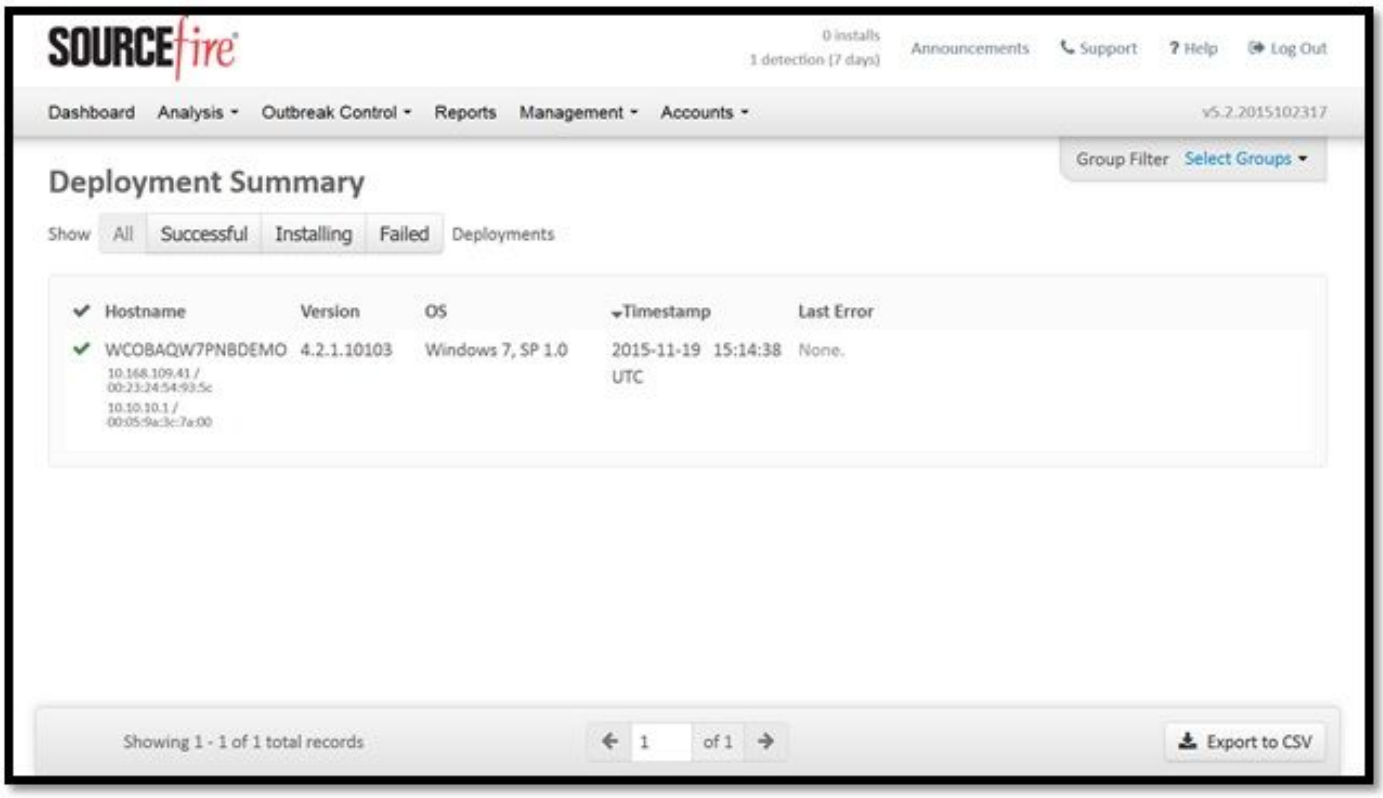
ステップ 8：コンピュータでの zip ファイルに含まれている Eicar 文字列を使用したテスト

すべてが予想通りはたらくかどうか確認するためにコンピュータの ZIP ファイルに示される Eicar ストリングとテストして下さい。



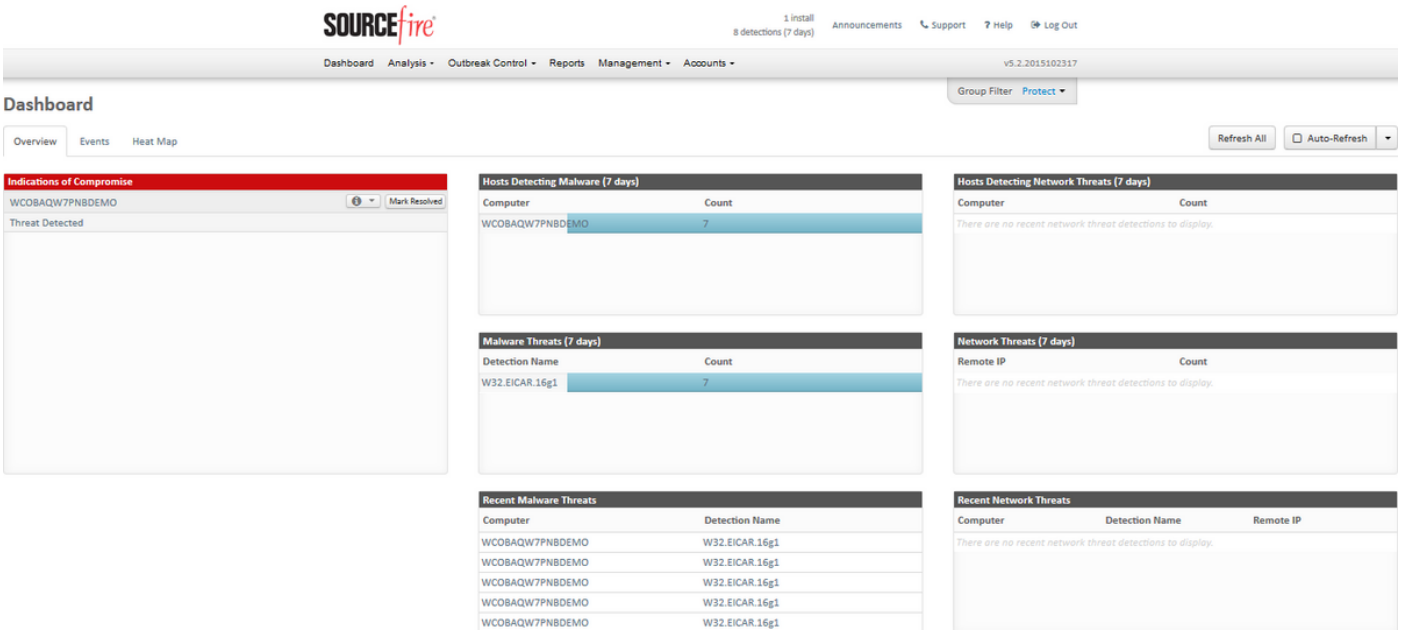
ステップ 9： 導入の概要

このページは成功したのリストが壊れる FireAMP コネクタ インストールする、また進行中のことを現在それら示し。 [Management] > [Deployment Summary] に移動できます。



ステップ 10： スレッド検出の検証

このページには、FireAMP Connector によりブロックされたスレッドと影響を受けるマシンのリストが表示されます。 [Dashboard] に移動できます。



追加情報

FireAMP Windows コネクタ用の対応しないソフトウェアは次のとおりです:

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

関連情報

- AMP イネーブラの設定
- テクニカルサポートとドキュメント - Cisco Systems