# Windows で動作する AMP for Endpoints コネクタからの診断データの収集

## 目次



## 概要

この資料は AMP for Endpoints コネクタからの診断ファイルを生成するためにステップを記述したものです。 Microsoft Windows で動作する AMP for Endpoints コネクタにおいての技術的な問題に直面すれば、Cisco テクニカルサポート エンジニアは診断ファイルで利用可能 な ログメッセージを分析したいと思うかもしれません。

## 診断ファイルの生成

Windowsのバージョンに依存は、AMP for Endpoints コネクタのサポート 診察道具へのナビゲーション異なるかもしれません。 ほとんどのウィンドウズオペレーティングシステムでは AMP for Endpoints コネクタのサポート 診察道具を見つけるために、Start メニューに行きます。 次に、例を示します。

**開始する > すべての Programs > Cisco AMP for Endpoints コネクタ > サポート 診察道具。**

> **注:** ユーザ アカウント制御を備えた Windows を実行している場合は、[Yes] をクリックしてツールを実行できるようにします。

Support Diagnostic Tool は、7z 形式の圧縮ファイルを生成してデスクトップに保存します。 この診断ツールがデスクトップに保存するファイル名の例は次のとおりです。

v5.0 およびそれ以前: `Sourcefire_Support_Tool_YYYY_MM_DD_HH_MM_SS.7z`

v5.1 : `CiscoAMP_Support_Tool_YYYY_MM_DD_HH_MM_SS.7z`

あるいは、管理者として以下の実行可能ファイルを実行することもできます。

```
v5.0 and earlier: C:\Program Files\Sourcefire\fireAMP\X.X.X\ipsupporttool.exe
v5.1 and newer: C:\Program Files\Cisco\AMP\X.X.X\ipsupporttool.exe
```

## デバッグ モード

AMP for Endpoints コネクタのデバッグ モードの Enablement はコネクタにおける問題により多

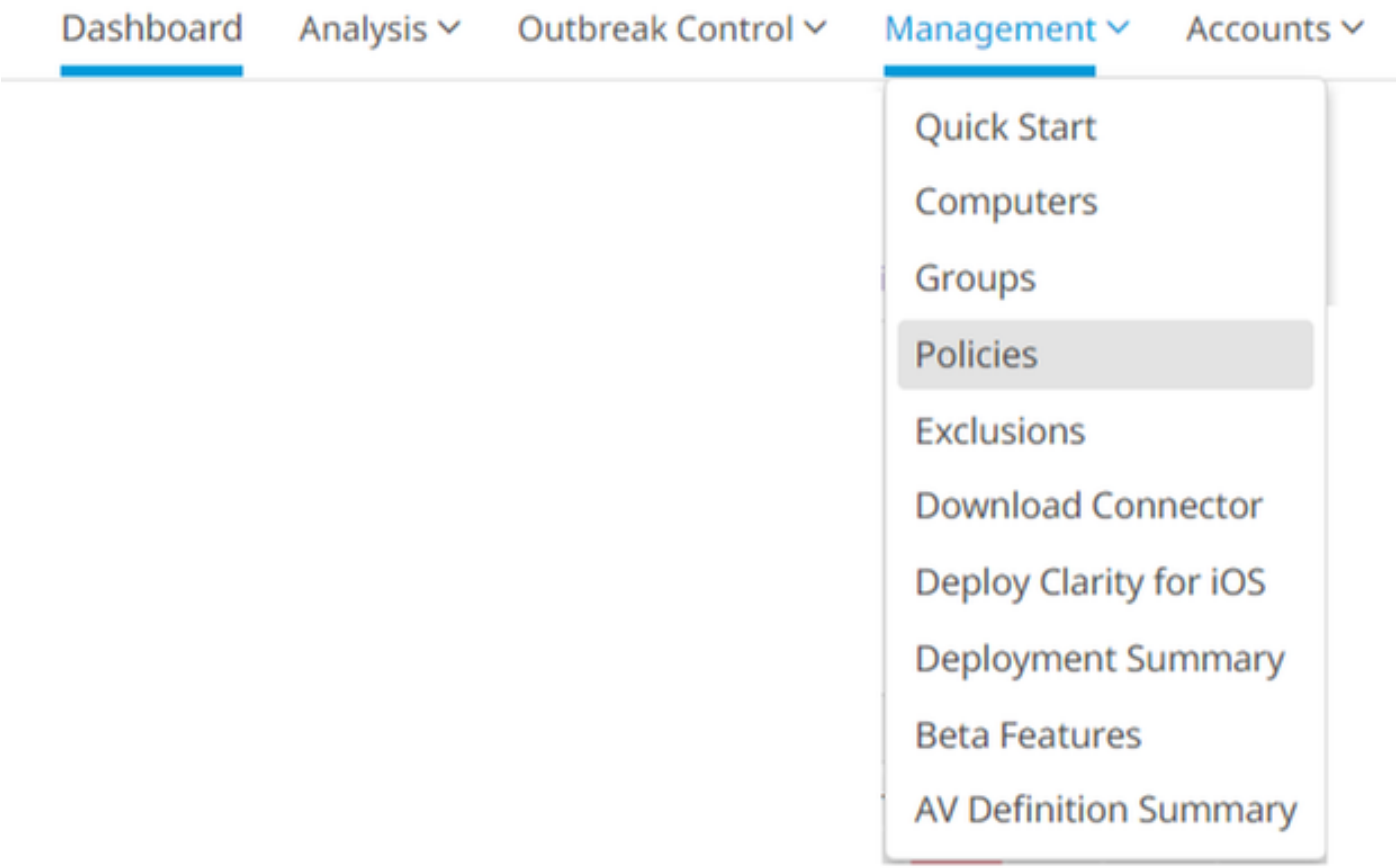
くの把握を割り当てるロギングに追加詳細を提供します。 このセクションは AMP for Endpoints コネクタのデバッグ モードを有効に する方法を記述します。

> **警告**： デバッグ モードを有効にするのは、シスコ テクニカル サポート エンジニアがデバッグ データを要請した場合に限ってください。 デバッグ モードを長時間にわたって有効にしていると、ディスク スペースがすぐにいっぱいになる可能性があります。さらに、**コネクタ ログ**と**トレイ ログ**のファイル サイズが大きくなりすぎて、Support Diagnostic Tool が生成するファイルに収集しきれなくなる場合もあります。

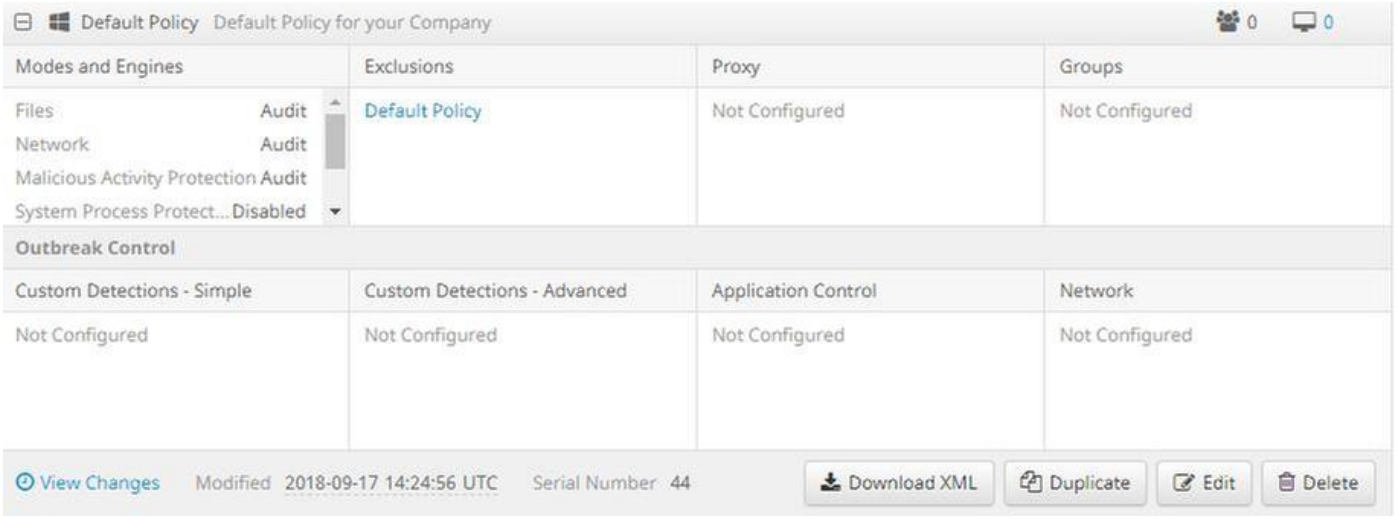
## デバッグ モードの有効化

ステップ 1： Cisco AMP for Endpoints コンソールにログイン して下さい。

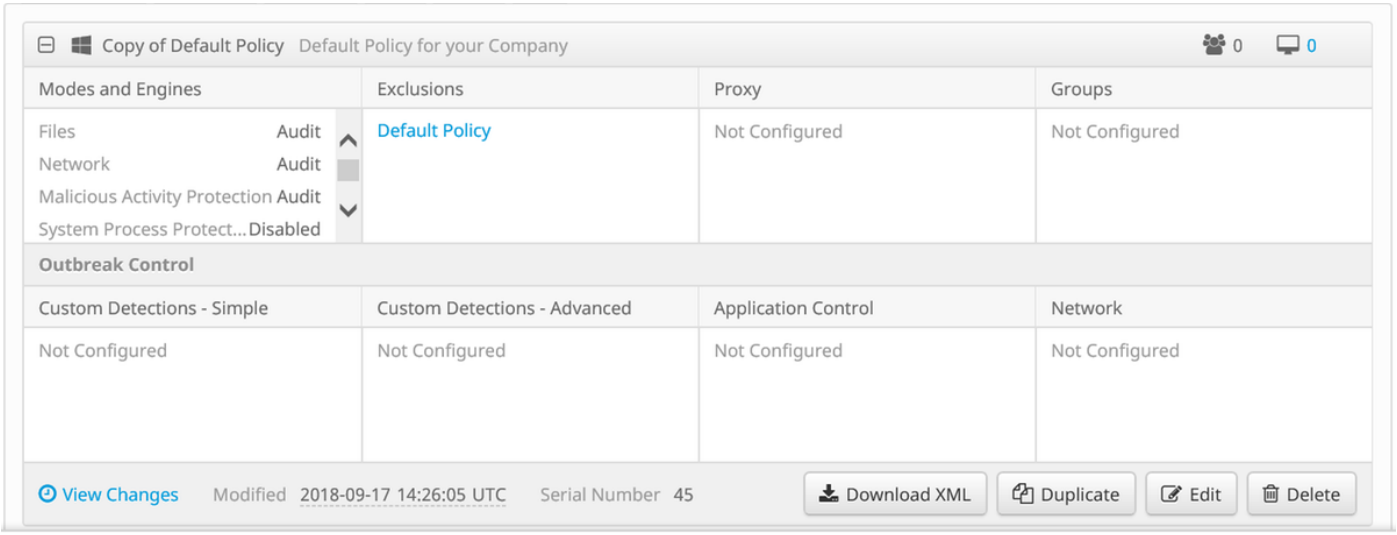
ステップ 2： [Management] > [Policies] を選択します。



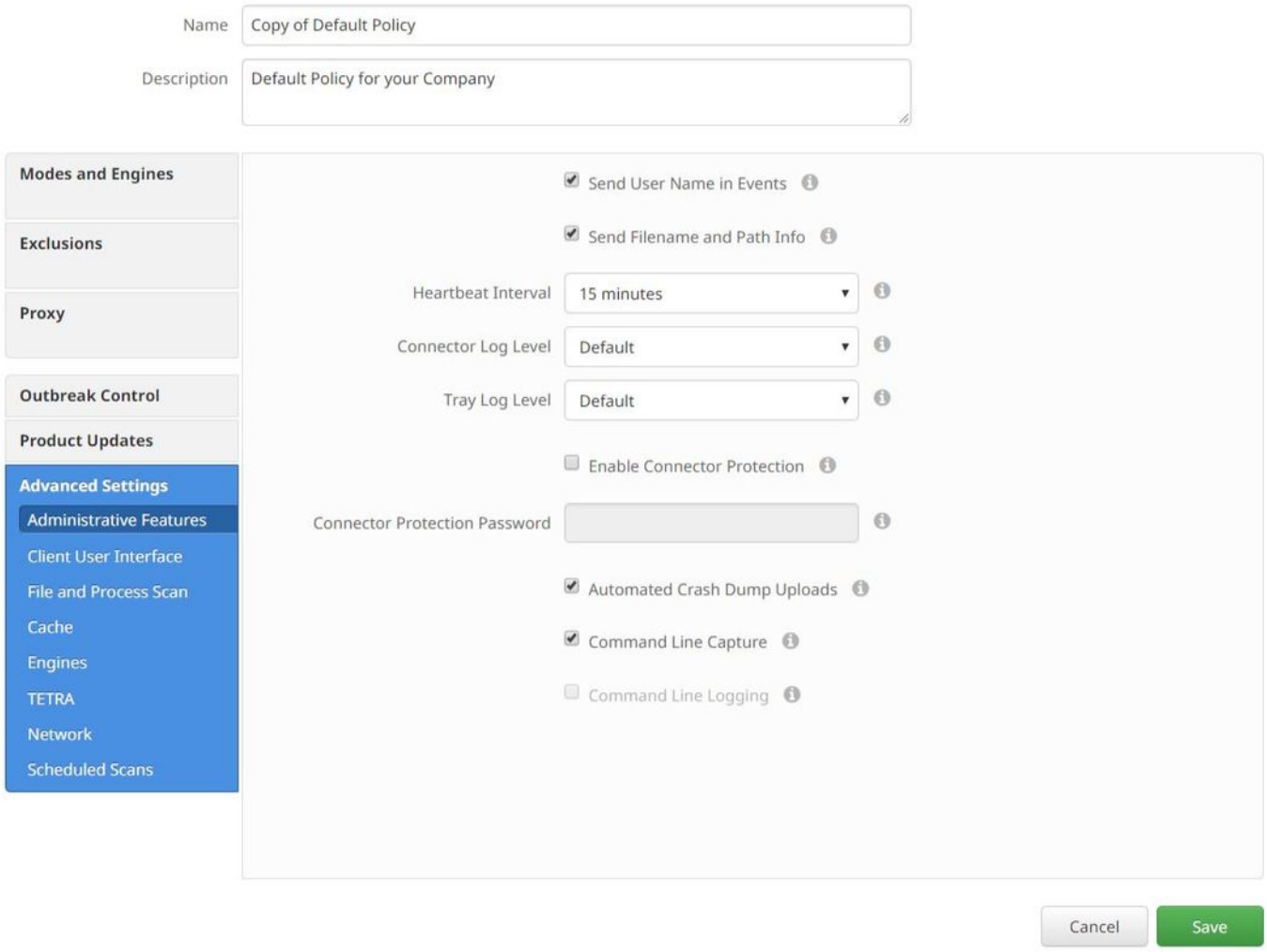

ステップ3： ポリシーをエンド デバイスかコンピュータに加えられる見つけ、**重複を**クリックして下さい。



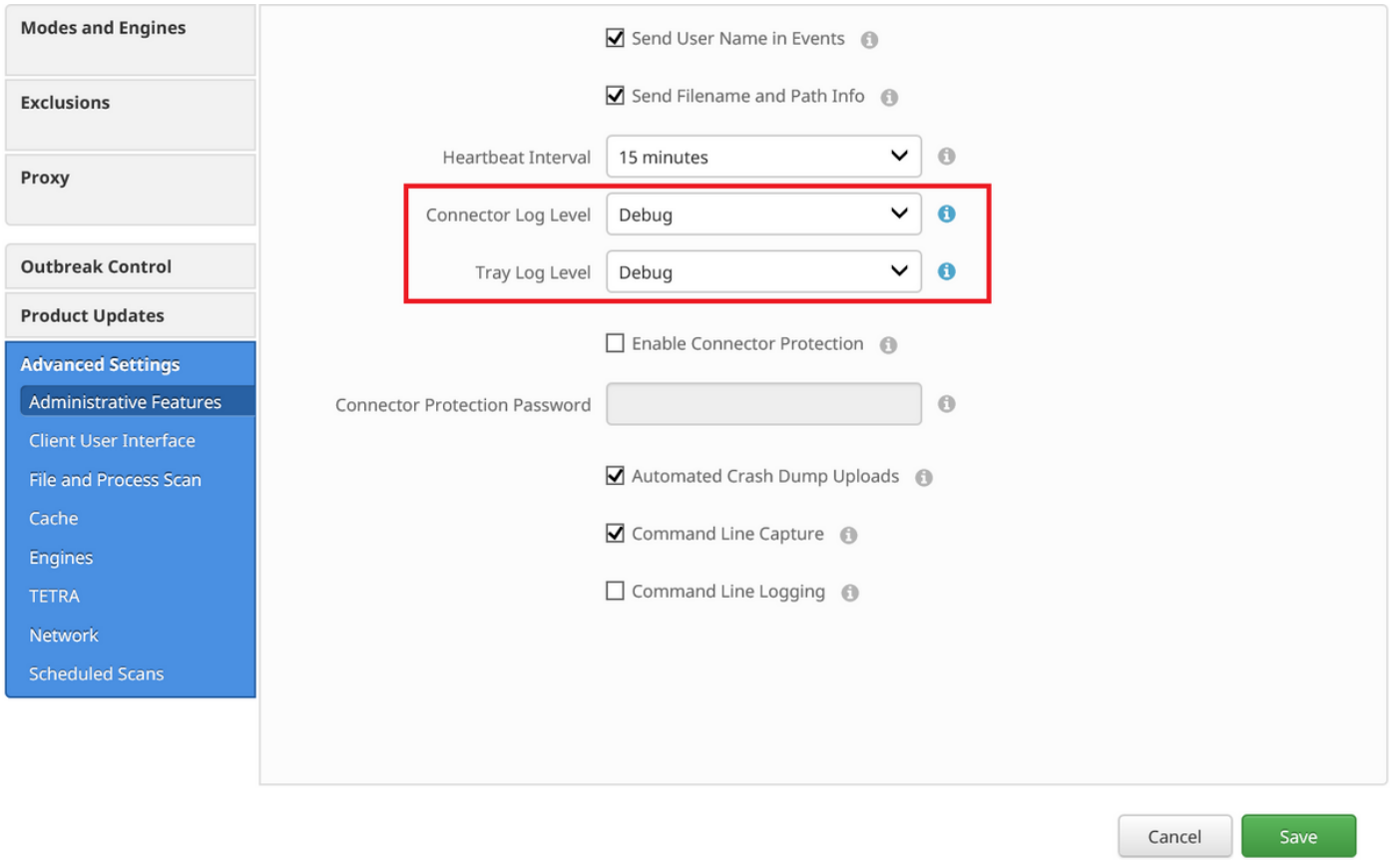

ステップ 4： 重複をクリックした後、複写されたポリシーの AMP for Endpoints コンソール更新 。



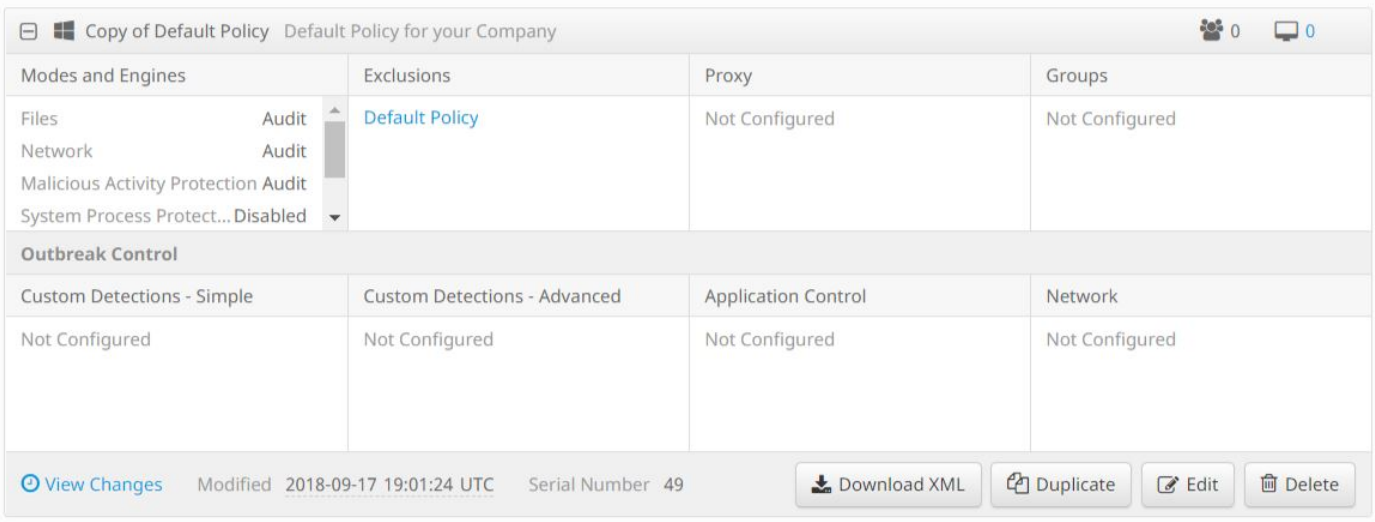

ステップ 5:Click は**設定 > 管理機能を編集し、**次に『Advanced』 をクリック します。




ステップ 6： [Tray Log Level] および [Connector Log Level] で、ドロップダウン リストから [Debug] を選択します。



ステップ 7： [Save] をクリックして変更を保存します。

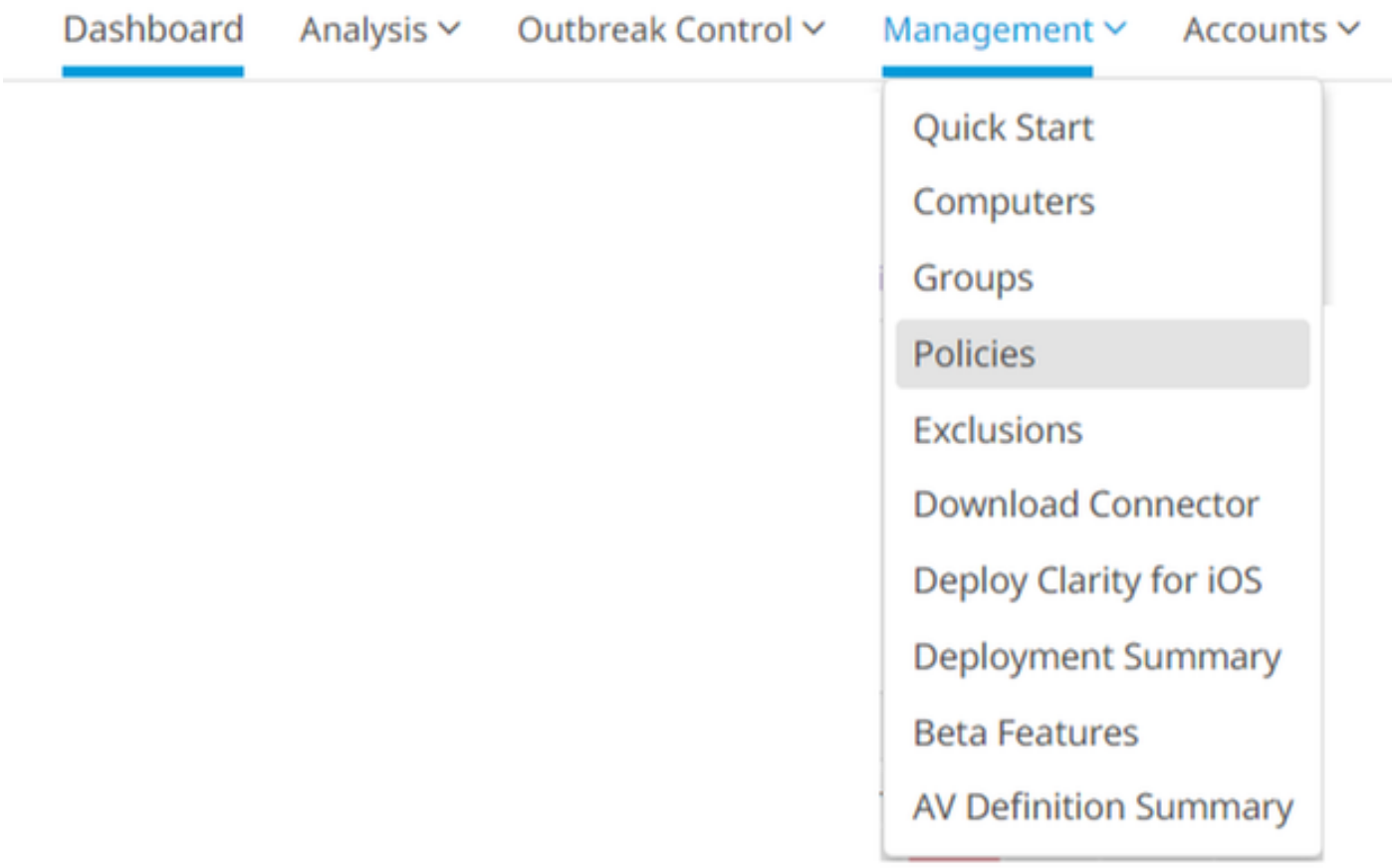



ステップ 8： ポリシーを更新した後、デバッグ情報を生成する対象のエンド デバイスに更新後のポリシーを適用する必要があります。

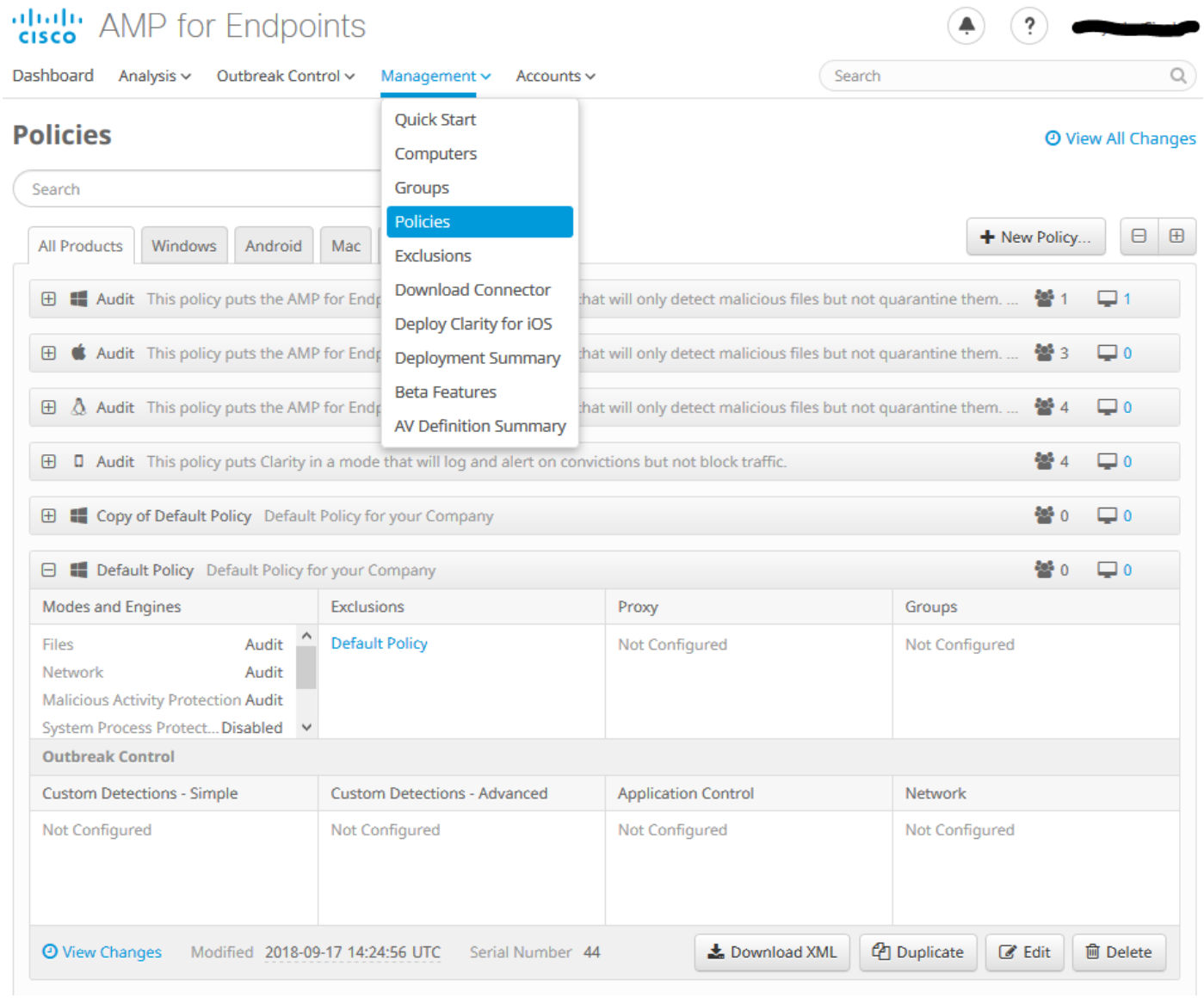
## デバッグ モードを有効にできない場合

AMP for Endpoints コネクタにポリシーを適用することができなければ接続上の問題が原因で、デバッグ モードを有効に することができません。 そのケースでは、`policy.xml` ダウンロードし、修正されたポリシーを使用するために AMP for Endpoints コネクタを設定できます。 AMP クラウドが AMP for Endpoints コネクタと通信することができない場合これらの手順に従って下さい:

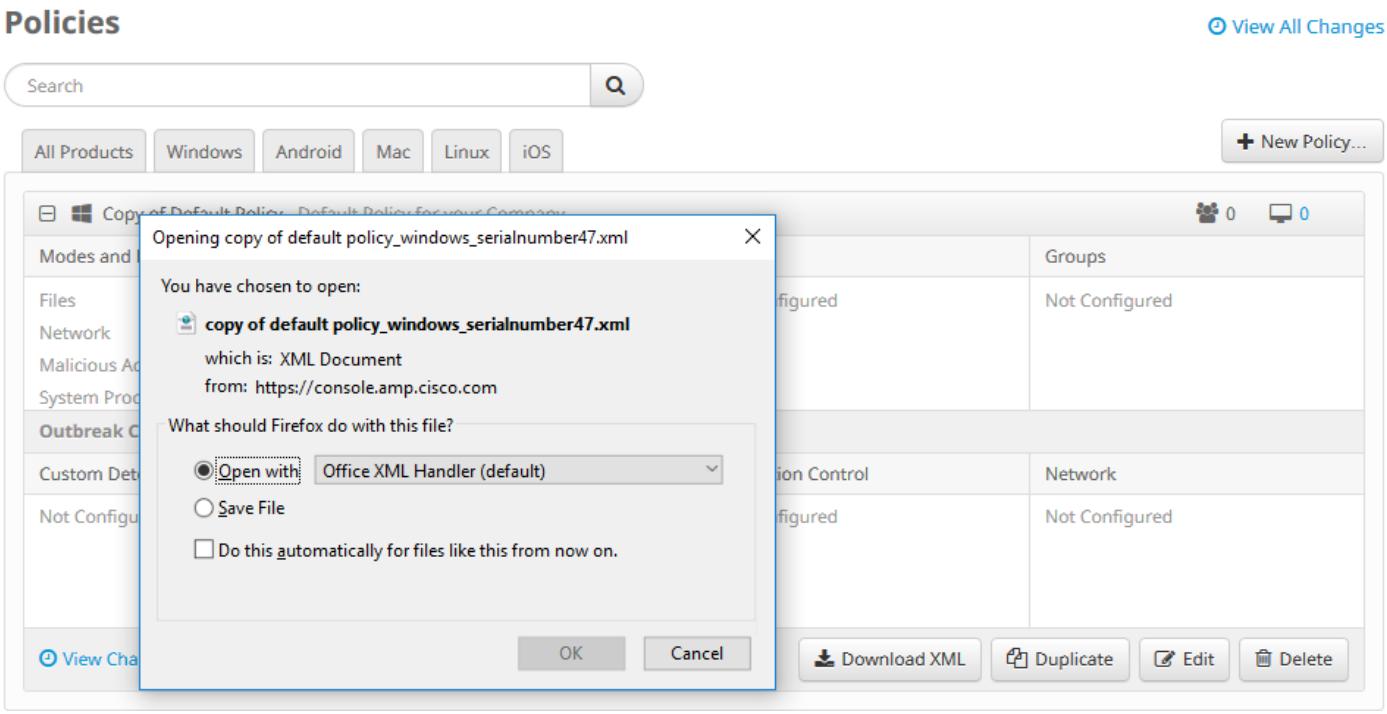
ステップ 1： [Management] > [Policies] を選択します。



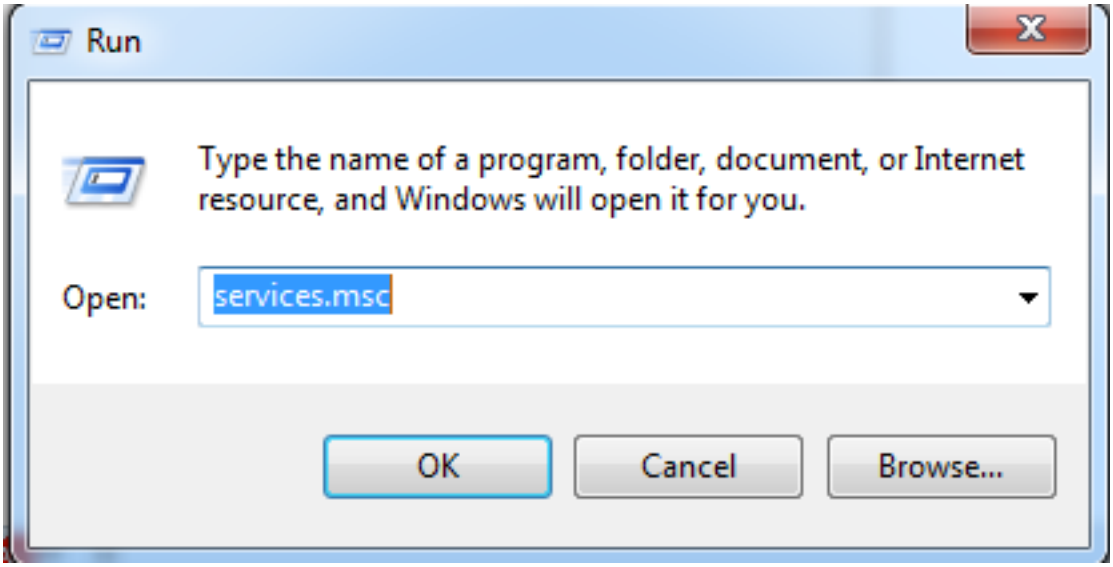
ステップ 2： コピーしたポリシーを見つけて、その名前をクリックします。これにより、[Policy Summary] が表示されます。



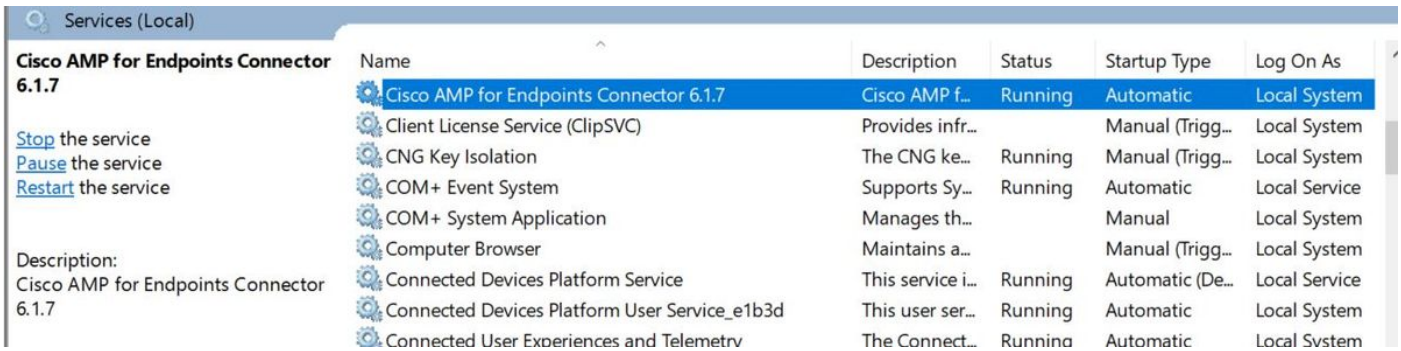

ステップ3： [Download Policy XML File] をクリックし、コンピュータにファイルを保存します。




ステップ 4： [Start] > [Run] を使用して **services.msc** . を開きます。




ステップ 5： **Cisco AMP for Endpoints コネクタ** サービスを見つけ、『Stop』 をクリック して下さい。




ステップ 6： [Start] > [Computer] をクリックし、コンピュータ アーキテクチャに応じて次のいずれかのディレクトリに移動します。

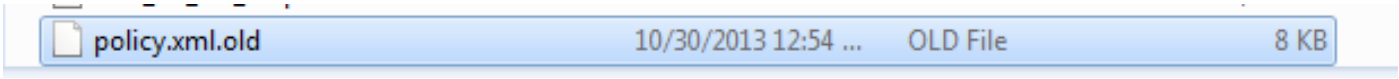
x86 プラットフォームの場合：

```
v5.0 and earlier: C:\Program Files (x86)\Sourcefire\fireAMP
v5.1 and newer: C:\Program Files (x86)\Cisco\AMP
```

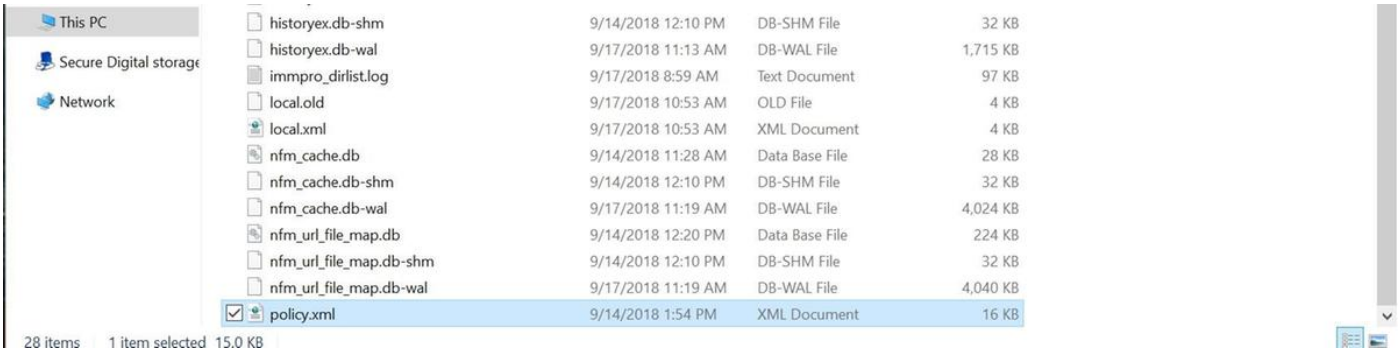
x64 プラットフォームの場合：

```
v5.0 and earlier: C:\Program Files\Sourcefire\fireAMP
v5.1 and newer: C:\Program Files\Cisco\AMP
```

ステップ 7： policy.xml ファイルを見つけて、その名前を policy.xml.old に変更します。




ステップ 8： ダウンロードした policy.xml をこのディレクトリに移動し、[Services] ウィンドウで [Start the service] をクリックします。 このとき AMP for Endpoints コネクタはデバッグ モードで、追加診断データを記録 します。




デバッグ モードを無効に するために、ステップ 5 からステップ 8 を実行し、`policy.xml.old` への変更を取消しAMP for Endpoints コネクタを。