Windows 上で動作する FireAMP コネクタからの診断データの収集

目次

概要

このドキュメントでは、FireAMP コネクタから診断ファイルを生成する手順を説明します。 Microsoft Windows 上で動作する FireAMP コネクタで技術的な問題が発生した場合、シスコ テクニカル サポート エンジニアが診断ファイルに含まれるログ メッセージを分析しなければならない場合があります。

診断ファイルの生成

Windows のバージョンによって、FireAMP コネクタの Support Diagnostic Tool に移動する方法は異なる場合があります。 ほとんどの Windows オペレーティング システムでは、[Start] メニューに移動すると FireAMP コネクタの Support Diagnostic Tool が見つかります。 次に、例を示します。

[Start] > [All Programs] > [FireAMP Connector] > [Support Diagnostic Tool]

> **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

FireAMP コネクタでデバッグ モードを有効にすると、ログにさらに詳細な情報が記録され、コネ

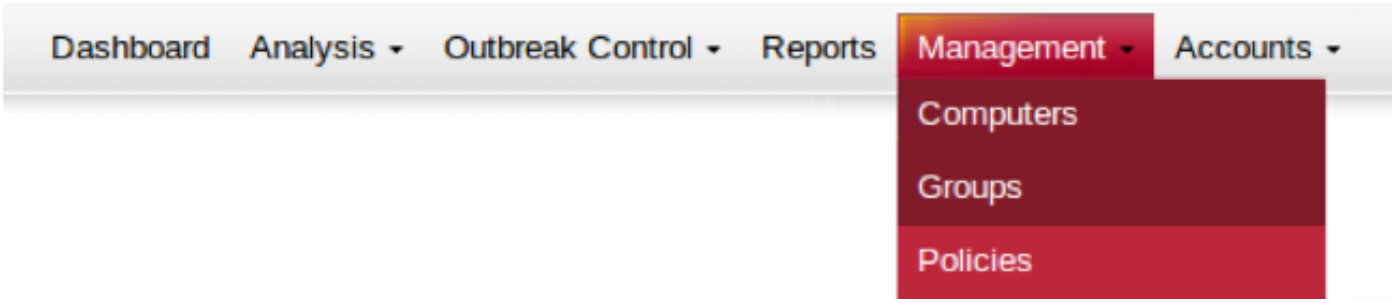
クタでの問題をより明確に理解できるようになります。 このセクションでは、FireAMP コネクタでデバッグ モードを有効にする方法を説明します。

> **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

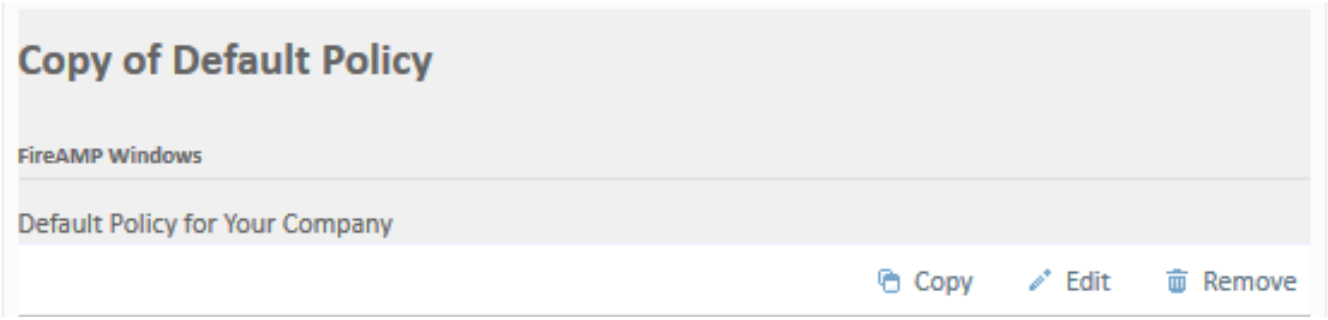
ステップ 1： FireAMP のコンソールにログインします。

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

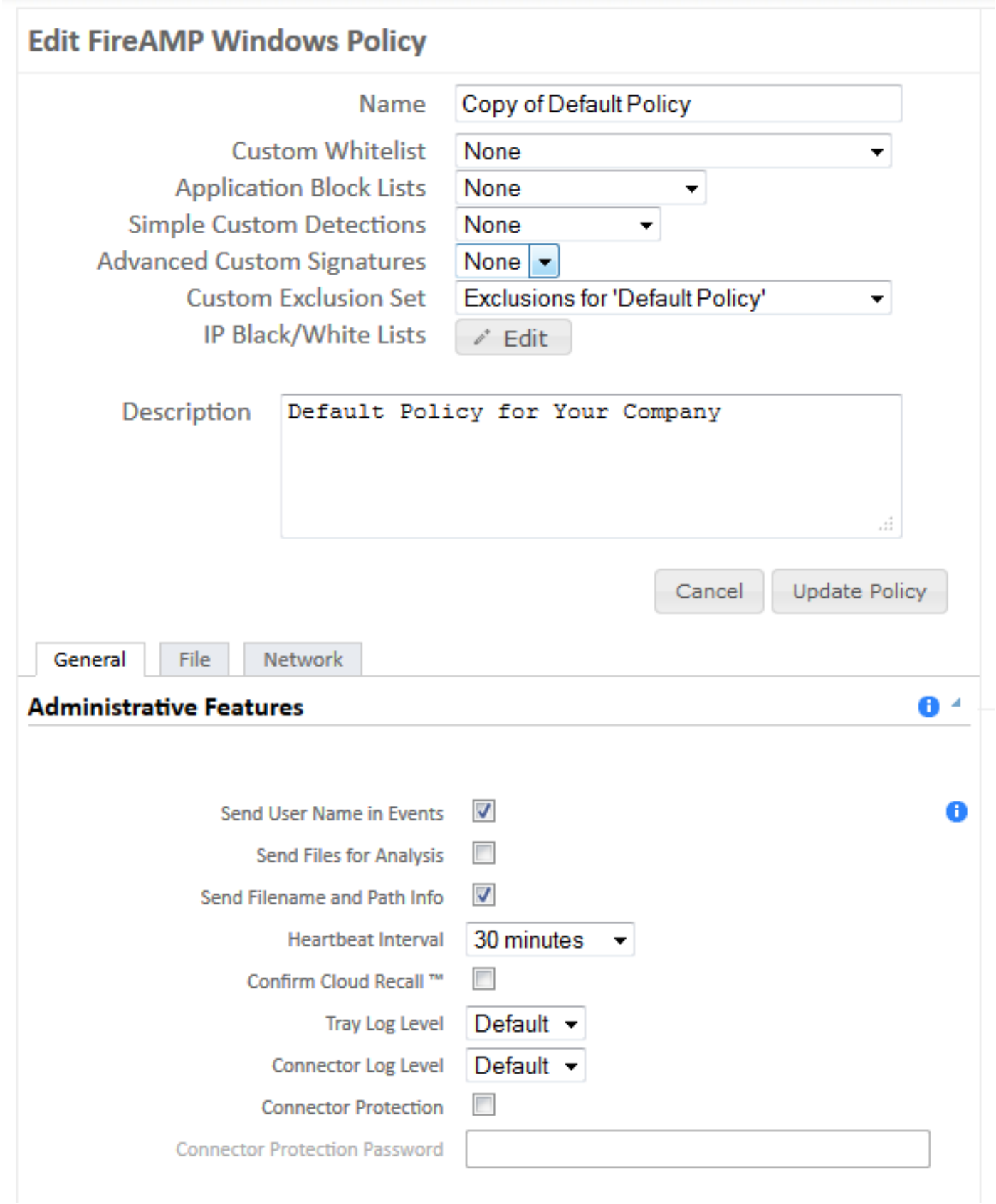


ステップ3： エンド デバイスまたはコンピュータに適用されているポリシーを見つけて、[Copy] をクリックします。.

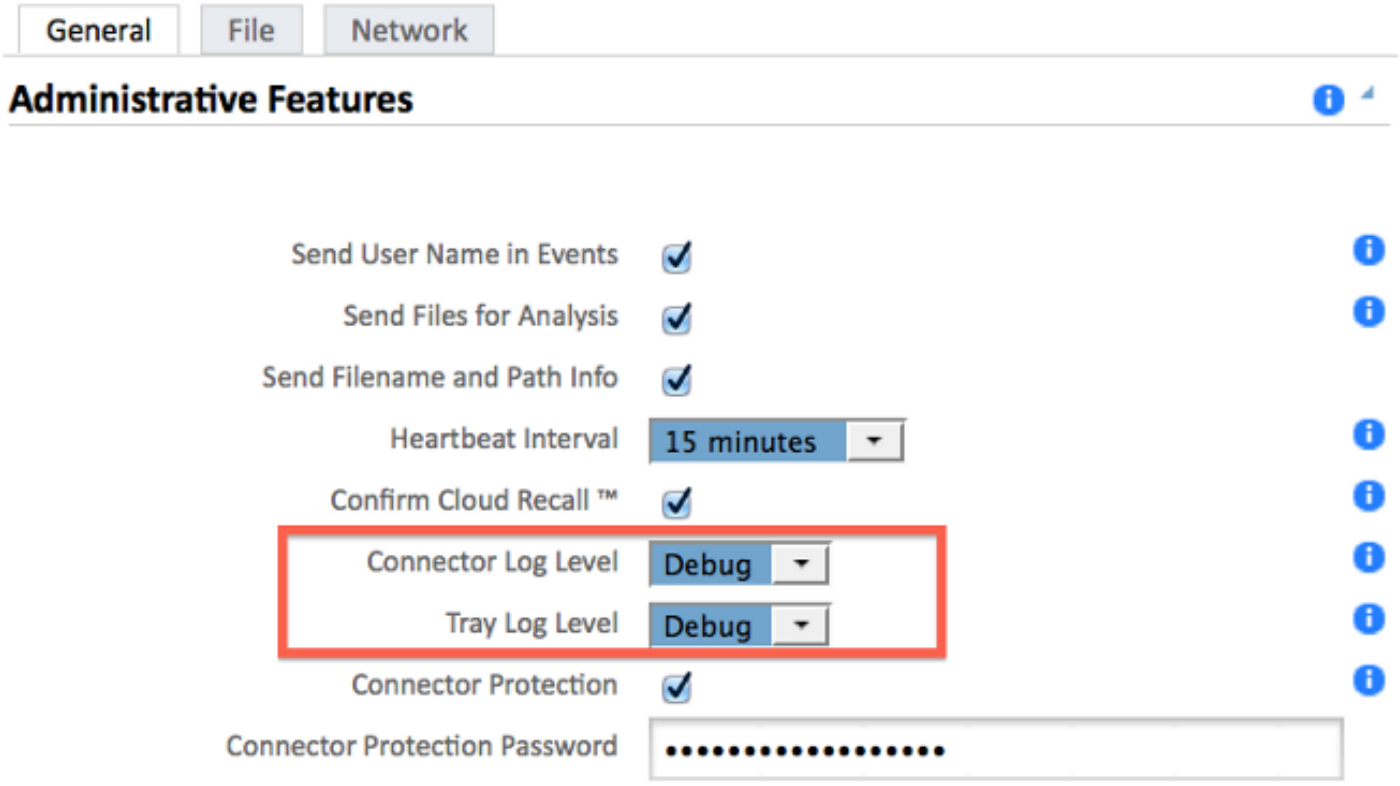
ステップ 4： [Copy] をクリックすると、FireAMP のコンソールがコピーされたポリシーで更新されます。



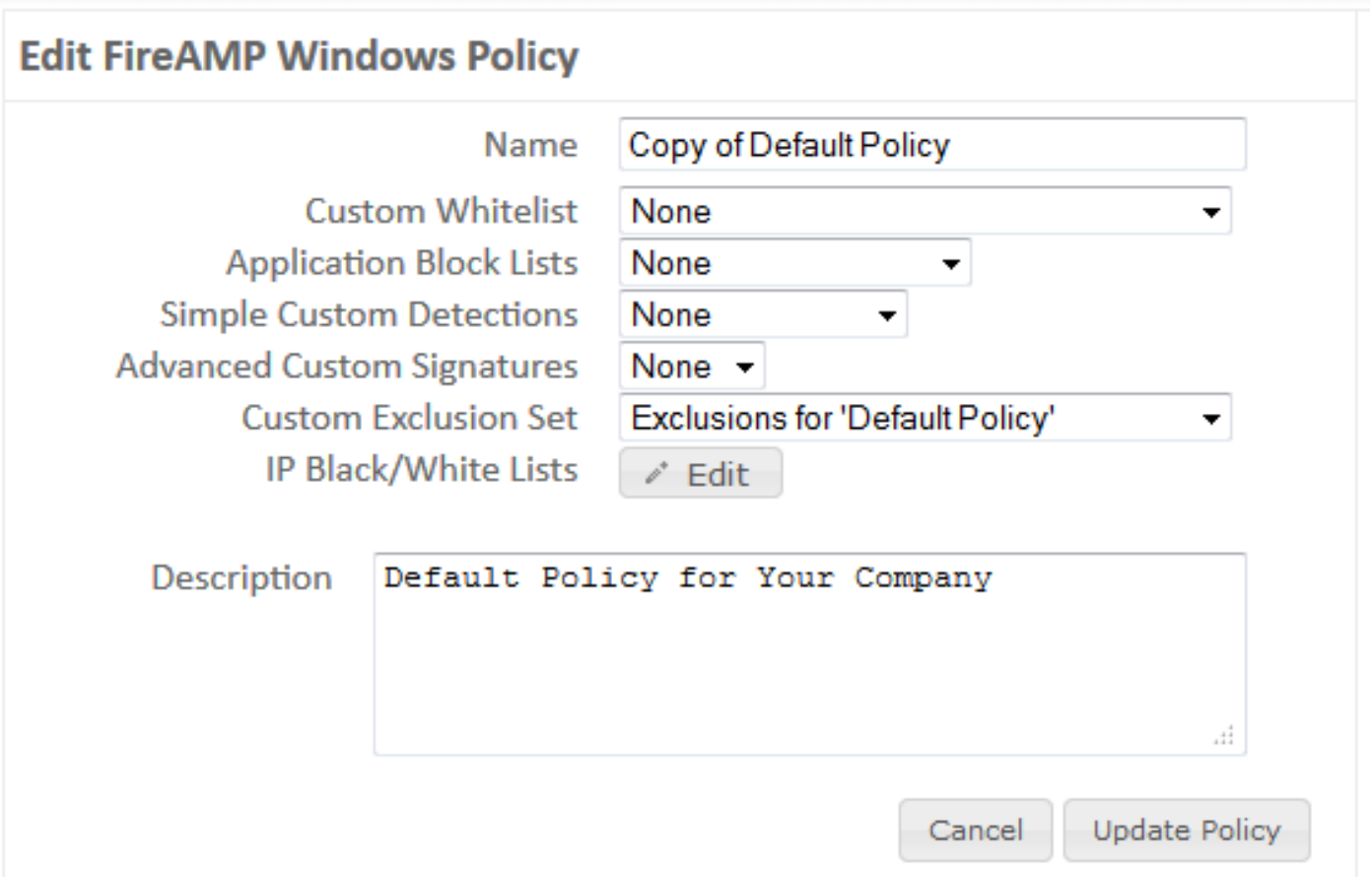
ステップ 5：[Edit]、[Administrative Features] の順にクリックします。



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： [Update Policy] をクリックして変更を保存します。

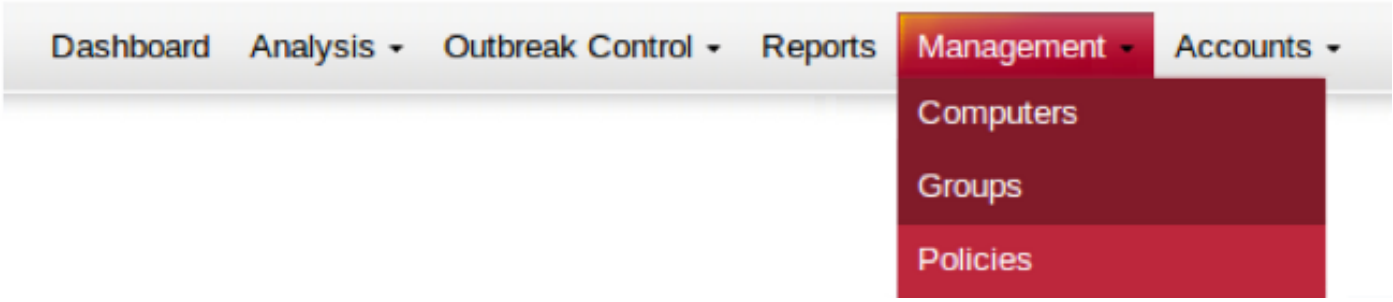


ステップ 8： ポリシーを更新した後、デバッグ情報を生成する対象のエンド デバイスに更新後のポリシーを適用する必要があります。

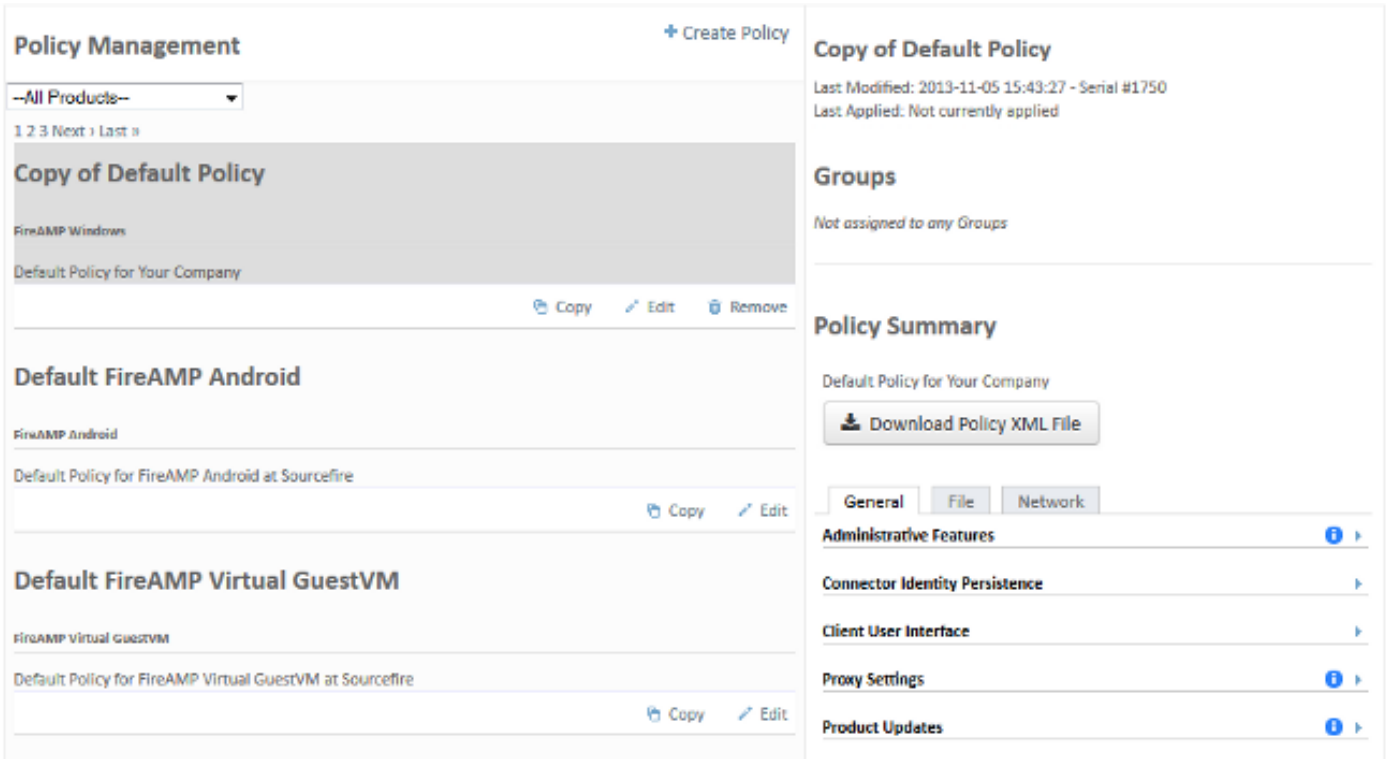
デバッグ モードを有効にできない場合

接続の問題が原因でポリシーを FireAMP コネクタに適用できない場合は、デバッグ モードを有効にできません。 その場合、policy.xml ファイルをダウンロードして、変更後のポリシーを使用するように FireAMP コネクタを設定します。 FireAMP クラウドが FireAMP コネクタと通信できない場合は、次の手順に従います。

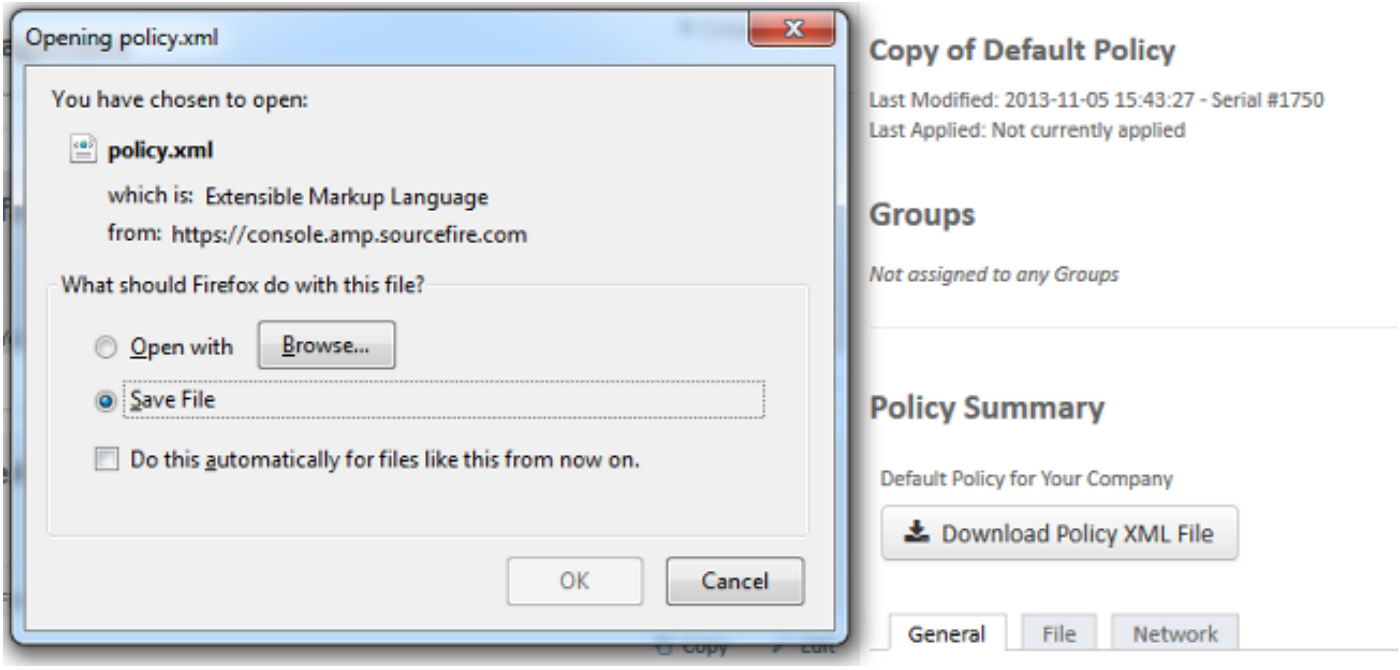
ステップ 1： [Management] > [Policies] を選択します。



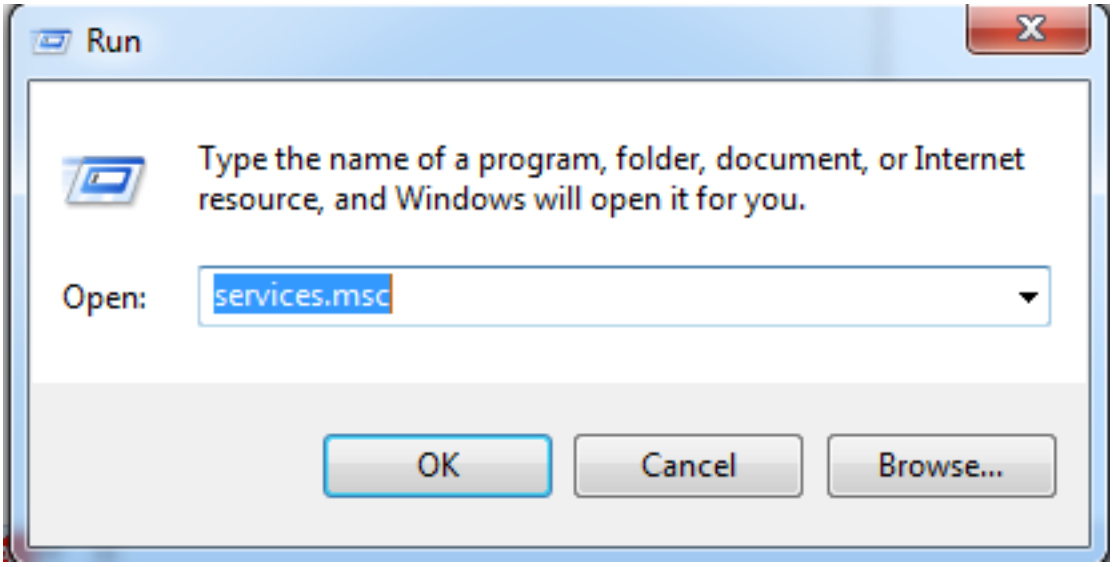
ステップ 2： コピーしたポリシーを見つけて、その名前をクリックします。これにより、[Policy Summary] が表示されます。



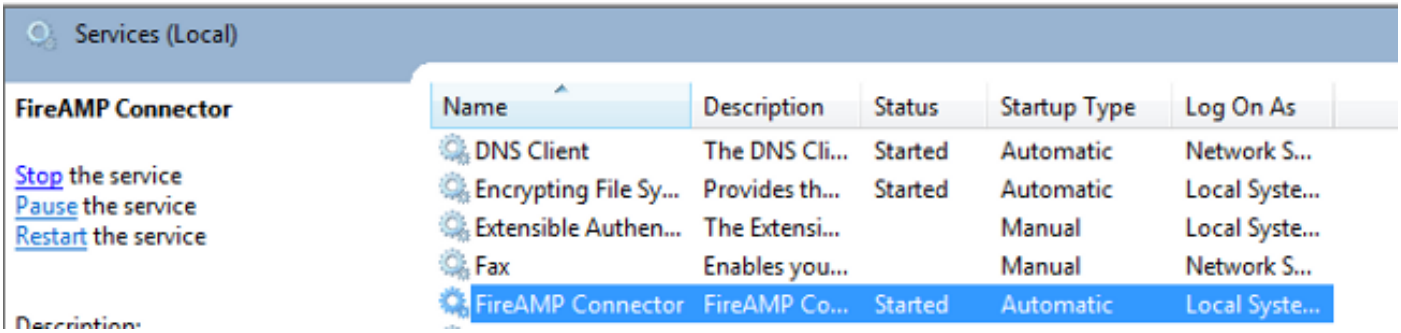
ステップ3： [Download Policy XML File] をクリックし、コンピュータにファイルを保存します。



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



ステップ 5： [FireAMP Connector] サービスを見つけて、[Stop] をクリックします。



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。

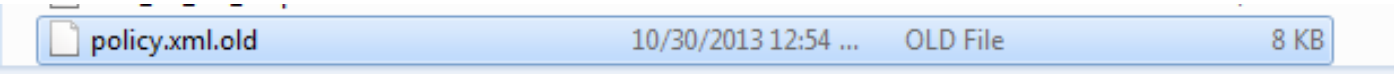
x86 プラットフォームの場合：

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

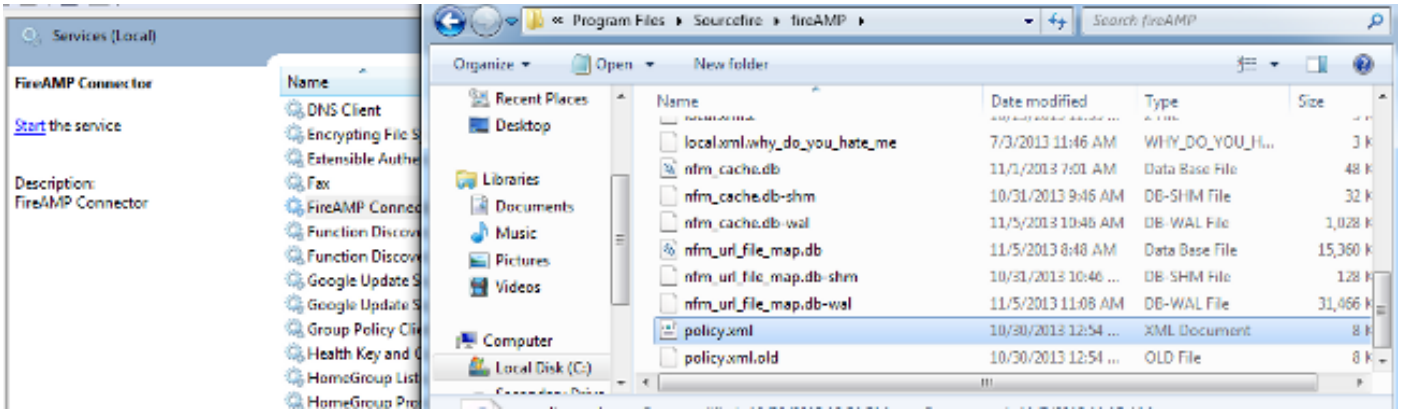
x64 プラットフォームの場合：

```
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。 FireAMP コネクタがデバッグ モードで詳細な診断データの記録を開始します。



デバッグ モードを無効にするには、ステップ 5 ～ 8 を実行して policy.xml.old の変更を元に戻した後、FireAMP コネクタを再起動します。