

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

[はじめに](#)

[診断ファイルの生成](#)

[デバッグ モード](#)

[デバッグ モードの有効化](#)

[デバッグ モードを有効にできない場合](#)

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

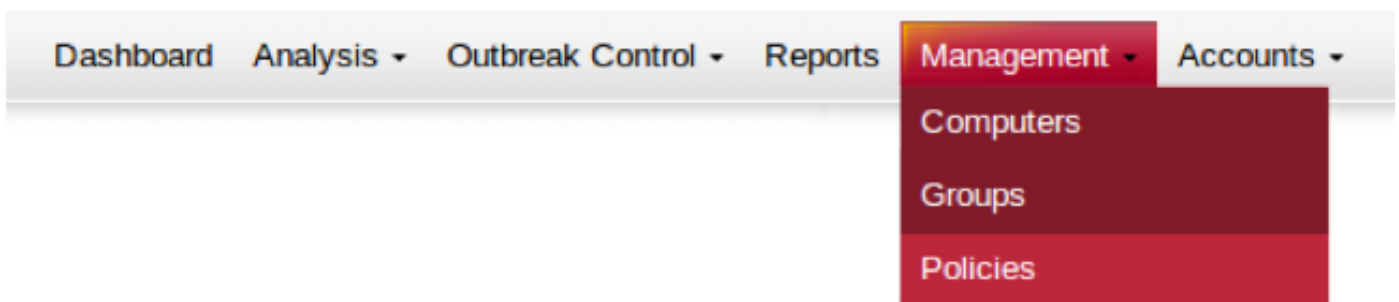
クタでの問題をより明確に理解できるようになります。このセクションでは、FireAMP コネクタでデバッグ モードを有効にする方法を説明します。

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。

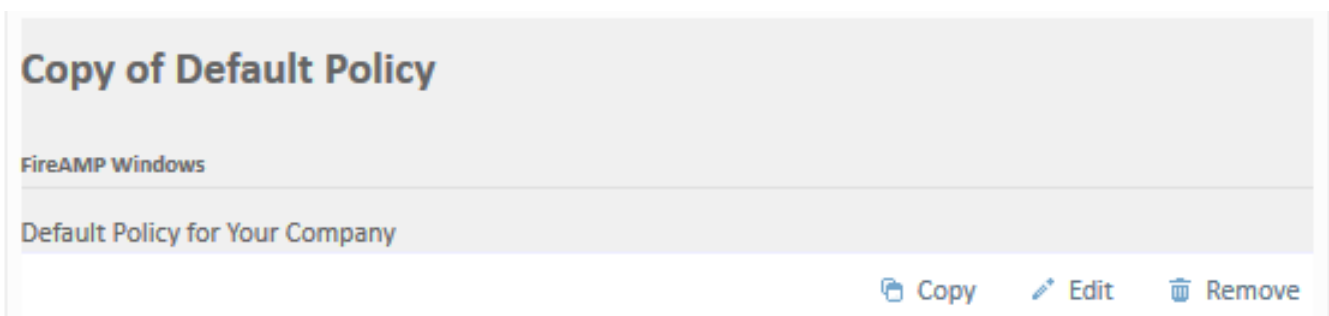
ステップ 2： [Management] > [Policies] を選択します。



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 findings に見つけて、[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。

Edit FireAMP Windows Policy

Name	<input type="text" value="Copy of Default Policy"/>
Custom Whitelist	<input type="text" value="None"/>
Application Block Lists	<input type="text" value="None"/>
Simple Custom Detections	<input type="text" value="None"/>
Advanced Custom Signatures	<input type="text" value="None"/>
Custom Exclusion Set	<input type="text" value="Exclusions for 'Default Policy'"/>
IP Black/White Lists	<input type="button" value="Edit"/>

Description	<input type="text" value="Default Policy for Your Company"/>
-------------	--

Administrative Features

Send User Name in Events	<input checked="" type="checkbox"/>	<input type="button" value="i"/>
Send Files for Analysis	<input type="checkbox"/>	
Send Filename and Path Info	<input checked="" type="checkbox"/>	
Heartbeat Interval	<input type="text" value="30 minutes"/>	
Confirm Cloud Recall™	<input type="checkbox"/>	
Tray Log Level	<input type="text" value="Default"/>	
Connector Log Level	<input type="text" value="Default"/>	
Connector Protection	<input type="checkbox"/>	
Connector Protection Password	<input type="text"/>	

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。

General

File

Network

Administrative Features



Send User Name in Events	<input checked="" type="checkbox"/>	
Send Files for Analysis	<input checked="" type="checkbox"/>	
Send Filename and Path Info	<input checked="" type="checkbox"/>	
Heartbeat Interval	15 minutes	
Confirm Cloud Recall™	<input checked="" type="checkbox"/>	
Connector Log Level	Debug	
Tray Log Level	Debug	
Connector Protection	<input checked="" type="checkbox"/>	
Connector Protection Password	

ステップ 7 : [Update Policy] をクリックして変更を保存します。

Edit FireAMP Windows Policy

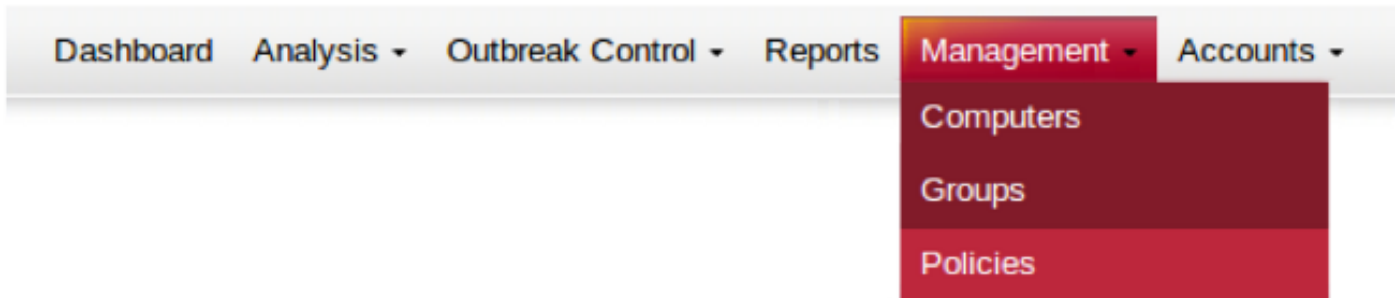
Name	Copy of Default Policy
Custom Whitelist	None
Application Block Lists	None
Simple Custom Detections	None
Advanced Custom Signatures	None
Custom Exclusion Set	Exclusions for 'Default Policy'
IP Black/White Lists	Edit
Description	Default Policy for Your Company

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。

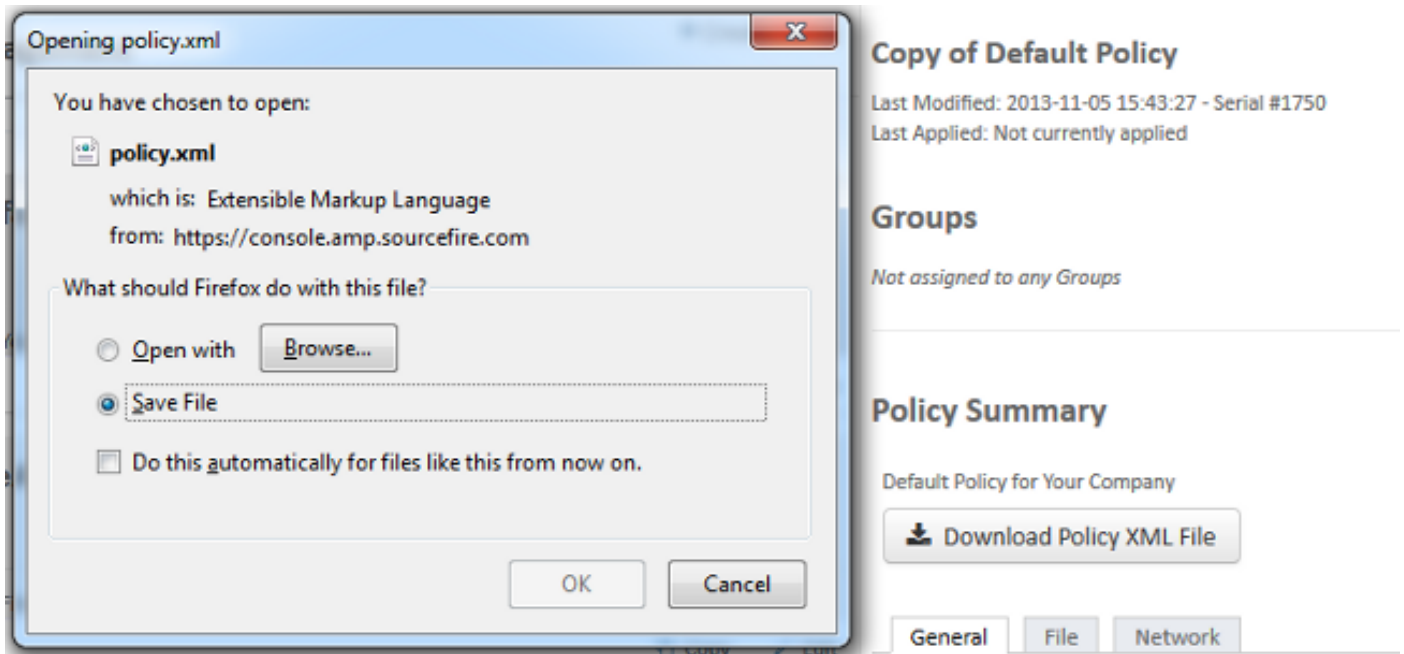
ステップ 1 : [Management] > [Policies] を選択します。



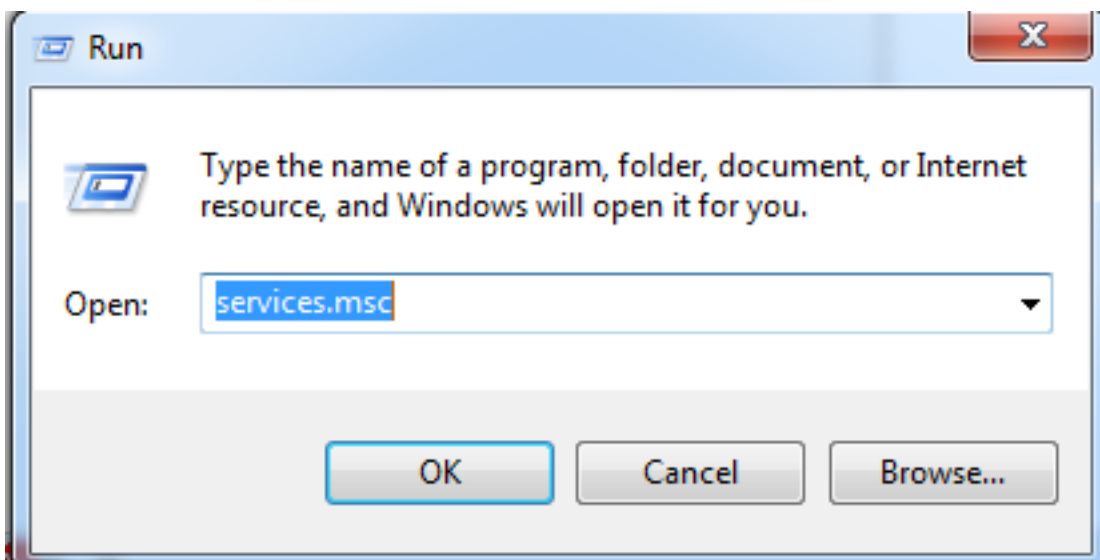
ステップ 2 : コピーしたポリシーをみつけて、その名前をクリックします。これにより、[Policy Summary] が表示されます。

A screenshot of the FireAMP Policy Management interface. On the left, a list of policies is shown under the heading 'Policy Management'. The policies listed are 'Copy of Default Policy', 'Default FireAMP Android', and 'Default FireAMP Virtual GuestVM'. The 'Copy of Default Policy' is selected. On the right, the 'Copy of Default Policy' details are shown, including 'Last Modified: 2013-11-05 15:43:27 - Serial #1750' and 'Last Applied: Not currently applied'. Below this, there are sections for 'Groups' (Not assigned to any Groups) and 'Policy Summary'. The 'Policy Summary' section has tabs for 'General', 'File', and 'Network'. Under 'General', there are expandable sections for 'Administrative Features', 'Connector Identity Persistence', 'Client User Interface', 'Proxy Settings', and 'Product Updates'. A 'Download Policy XML File' button is visible in the 'Policy Summary' section.

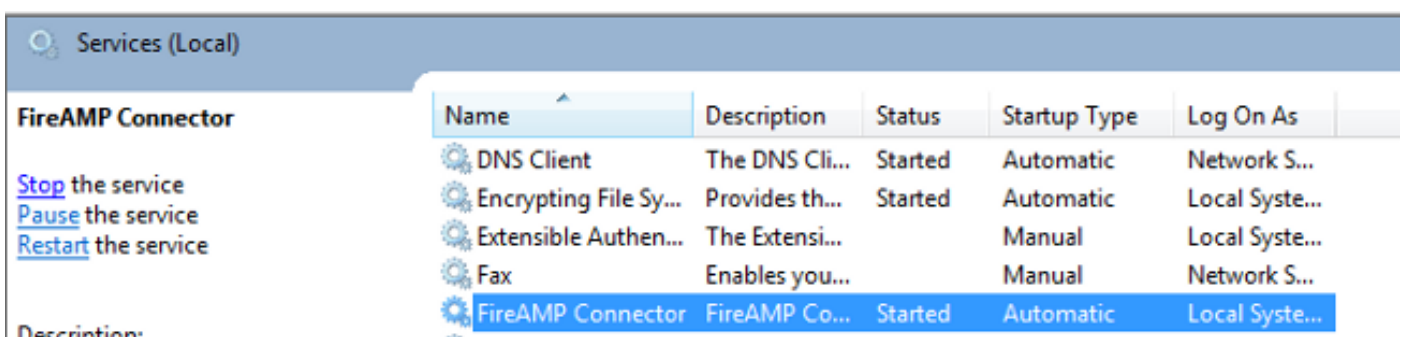
ステップ3 : [Download Policy XML File] をクリックし、コンピュータにファイルを保存します。



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

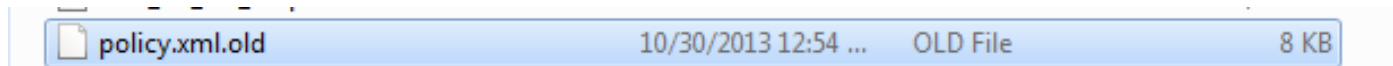
v5.1 and newer: C:\Program Files (x86)\Cisco\AMP

x64 プラットフォームの場合 :

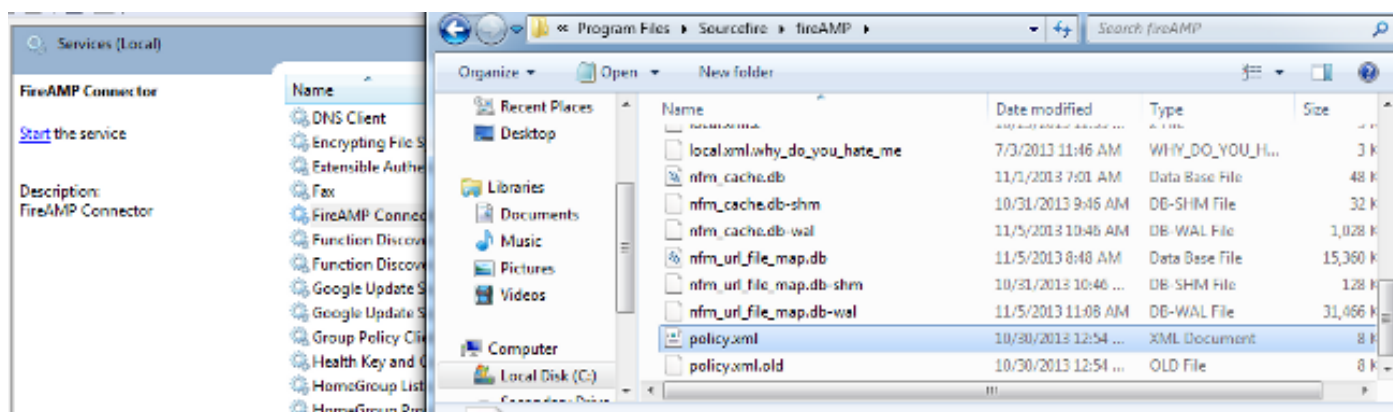
v5.0 and earlier: C:\Program Files\Sourcefire\fireAMP

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。