

# 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

[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 コネクタにつ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

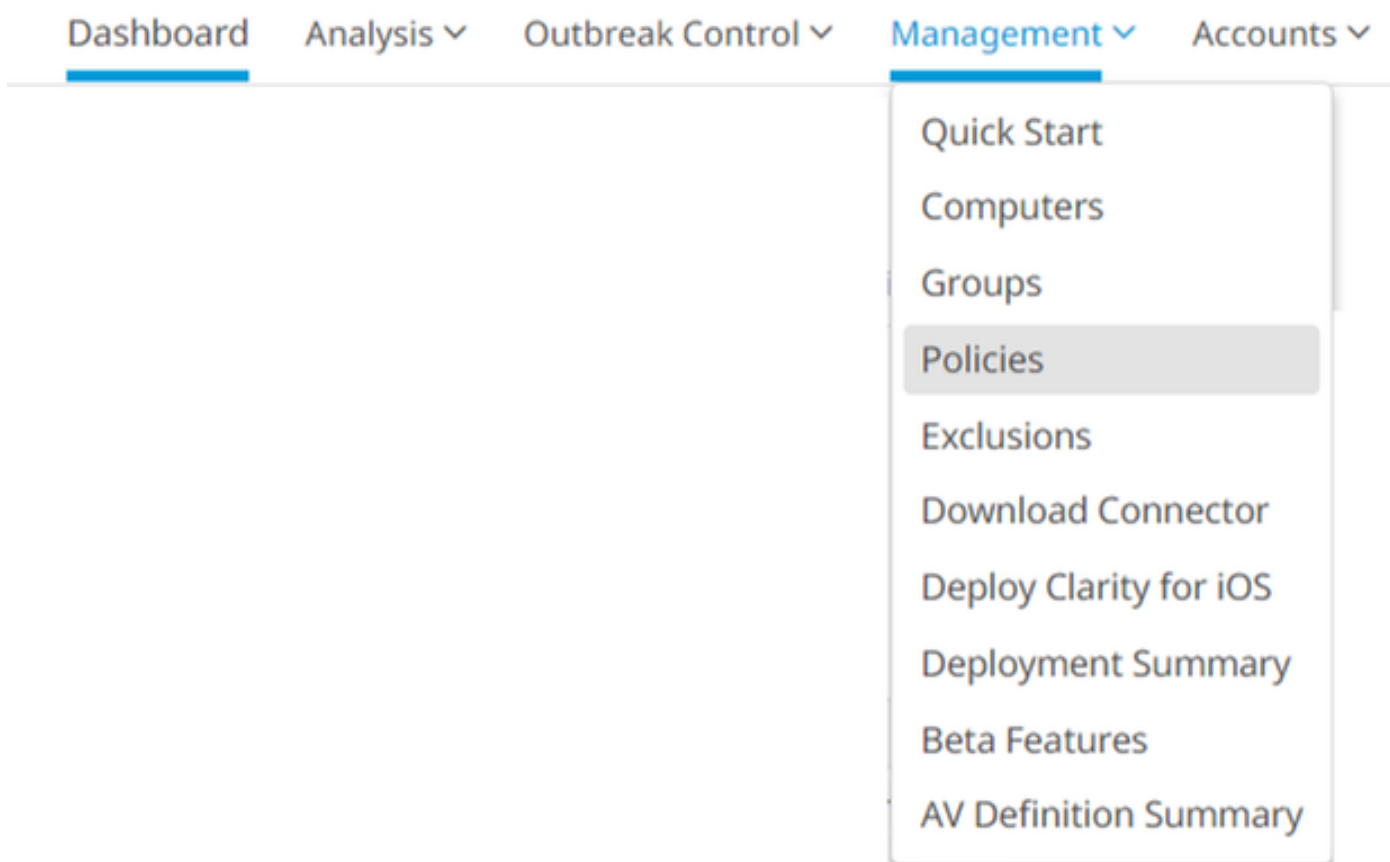
くの把握を割り当てるロギングに追加詳細を提供します。このセクションは AMP for Endpoints コネクタのデバッグ モードを有効にする方法を記述します。

**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。

Default Policy Default Policy for your Company

Modes and Engines	Exclusions	Proxy	Groups
Files Audit	Default Policy	Not Configured	Not Configured
Network Audit			
Malicious Activity Protection Audit			
System Process Protect... Disabled			
Outbreak Control			
Custom Detections - Simple	Custom Detections - Advanced	Application Control	Network
Not Configured	Not Configured	Not Configured	Not Configured

View Changes Modified 2018-09-17 14:24:56 UTC Serial Number 44

Download XML Duplicate Edit Delete

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

Copy of Default Policy Default Policy for your Company

Modes and Engines	Exclusions	Proxy	Groups
Files Audit	Default Policy	Not Configured	Not Configured
Network Audit			
Malicious Activity Protection Audit			
System Process Protect... Disabled			
Outbreak Control			
Custom Detections - Simple	Custom Detections - Advanced	Application Control	Network
Not Configured	Not Configured	Not Configured	Not Configured

View Changes Modified 2018-09-17 14:26:05 UTC Serial Number 45

Download XML Duplicate Edit Delete

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。

Name Copy of Default Policy

Description Default Policy for your Company

- Modes and Engines
- Exclusions
- Proxy
- Outbreak Control
- Product Updates
- Advanced Settings**
  - Administrative Features
  - Client User Interface
  - File and Process Scan
  - Cache
  - Engines
  - TETRA
  - Network
  - Scheduled Scans

Send User Name in Events ⓘ

Send Filename and Path Info ⓘ

Heartbeat Interval 15 minutes ⓘ

Connector Log Level Default ⓘ

Tray Log Level Default ⓘ

Enable Connector Protection ⓘ

Connector Protection Password ⓘ

Automated Crash Dump Uploads ⓘ

Command Line Capture ⓘ

Command Line Logging ⓘ

Cancel Save

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。

**Modes and Engines**

**Exclusions**

**Proxy**

**Outbreak Control**

**Product Updates**

**Advanced Settings**

- Administrative Features
- Client User Interface
- File and Process Scan
- Cache
- Engines
- TETRA
- Network
- Scheduled Scans

Send User Name in Events ⓘ

Send Filename and Path Info ⓘ

Heartbeat Interval 15 minutes ⓘ

**Connector Log Level Debug ⓘ**

**Tray Log Level Debug ⓘ**

Enable Connector Protection ⓘ

Connector Protection Password ⓘ

Automated Crash Dump Uploads ⓘ

Command Line Capture ⓘ

Command Line Logging ⓘ

Cancel Save

ステップ 7 : [Save] をクリックして変更を保存します。

The screenshot shows a web interface for configuring a policy. The title bar reads "Copy of Default Policy" and "Default Policy for your Company". The interface is divided into several sections:

- Modes and Engines:** A table with columns for the mode and its status. The modes listed are Files (Audit), Network (Audit), Malicious Activity Protection Audit, and System Process Protect... Disabled.
- Exclusions:** A section with a "Default Policy" link.
- Proxy:** A section with the status "Not Configured".
- Groups:** A section with the status "Not Configured".
- Outbreak Control:** A section with sub-sections: Custom Detections - Simple, Custom Detections - Advanced, Application Control, and Network. All are currently "Not Configured".

At the bottom, there is a status bar showing "Modified 2018-09-17 19:01:24 UTC" and "Serial Number 49". Action buttons include "View Changes", "Download XML", "Duplicate", "Edit", and "Delete".

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。

The screenshot shows the top navigation bar of the dashboard with the following items: Dashboard, Analysis, Outbreak Control, Management, and Accounts. The "Management" menu is open, showing a list of options: Quick Start, Computers, Groups, Policies (highlighted), Exclusions, Download Connector, Deploy Clarity for iOS, Deployment Summary, Beta Features, and AV Definition Summary.

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。

The screenshot shows the Cisco AMP for Endpoints Management interface. The 'Management' menu is open, and 'Policies' is selected. The main area displays a list of policies, including 'Audit' policies for Windows, Android, and Mac, and a 'Default Policy' for the company. The 'Default Policy' is expanded to show configuration details for Modes and Engines, Exclusions, Proxy, and Groups.

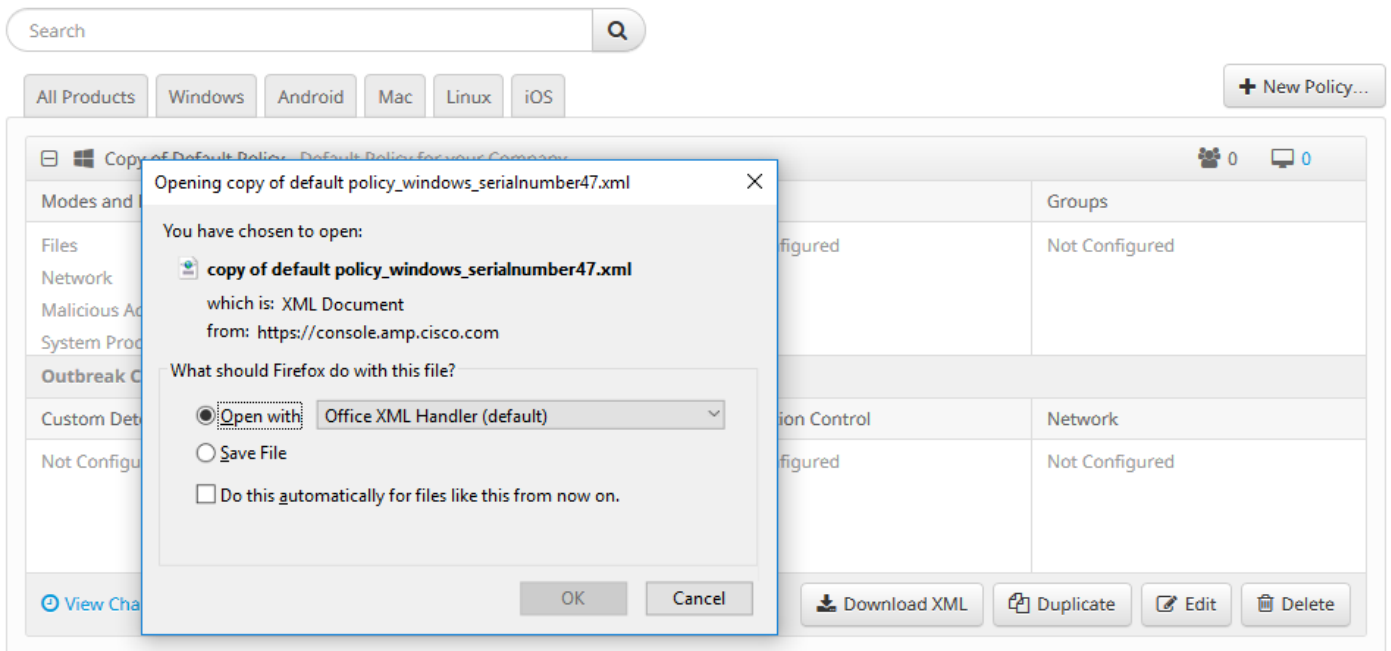
Modes and Engines	Exclusions	Proxy	Groups
Files Audit Network Audit Malicious Activity Protection Audit System Process Protect... Disabled	Default Policy	Not Configured	Not Configured

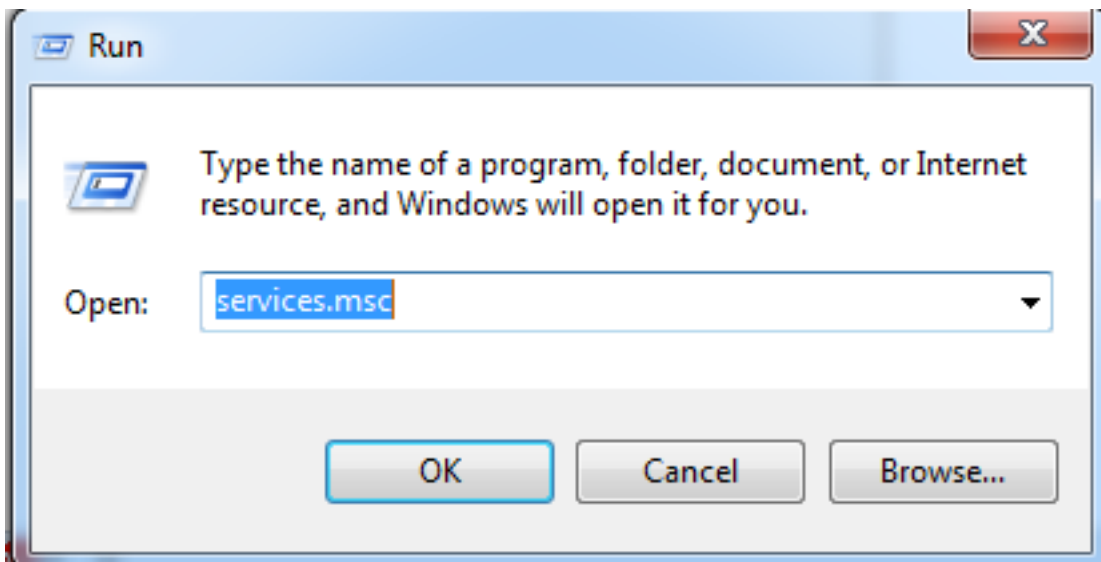
Outbreak Control			
Custom Detections - Simple	Custom Detections - Advanced	Application Control	Network
Not Configured	Not Configured	Not Configured	Not Configured

At the bottom of the expanded policy view, there are buttons for 'View Changes', 'Download XML', 'Duplicate', 'Edit', and 'Delete'. The 'Download XML' button is highlighted.

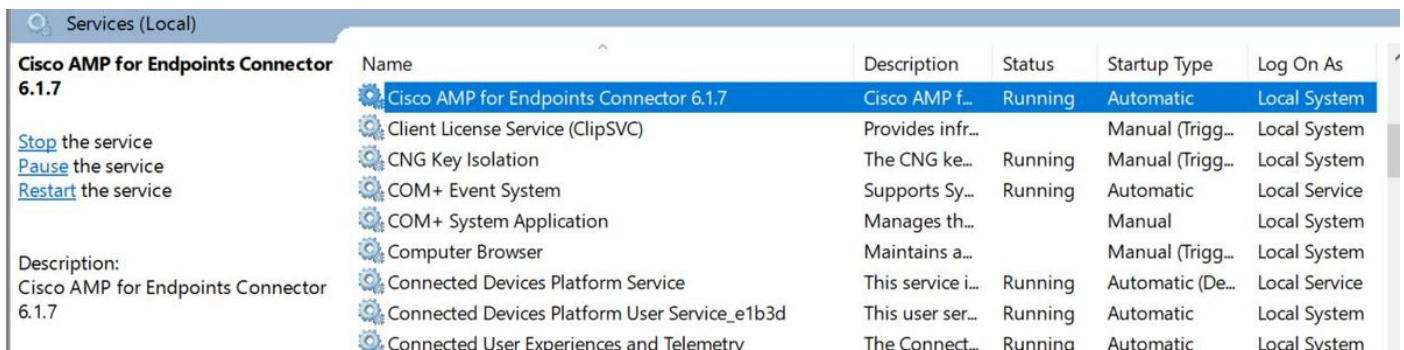
ステップ3：[Download Policy XML File]をクリックし、コンピュータにファイルを保存します。



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

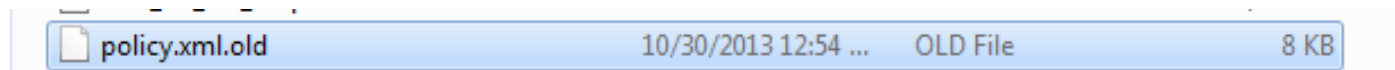
v5.1 and newer: C:\Program Files (x86)\Cisco\AMP

x64 プラットフォームの場合 :

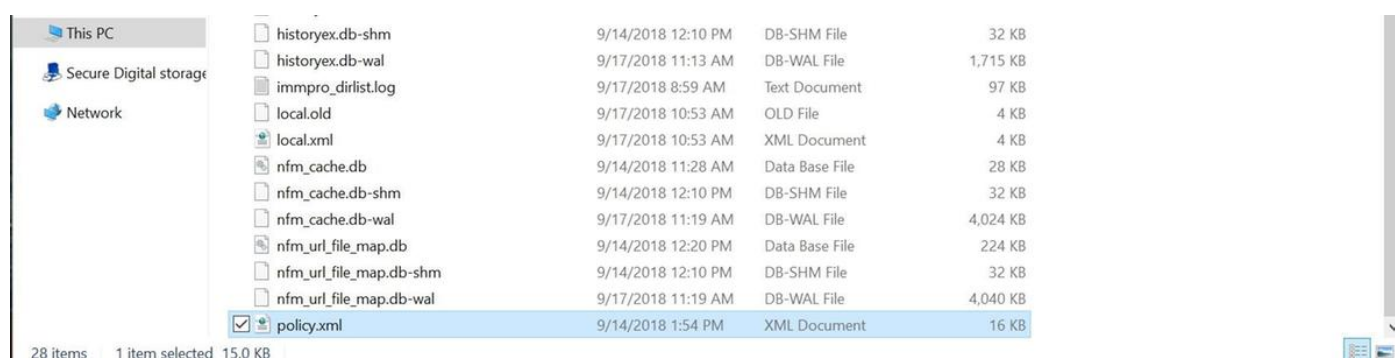
v5.0 and earlier: C:\Program Files\Sourcefire\fireAMP

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 への変更をキャンセルしAMP for Endpoints コネクタを。