

# 識別永続性の Cisco AMP for Endpoints の配備

## 目次

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[作業の流れ](#)

[設定](#)

[確認](#)

[トラブルシューティング](#)

[関連情報](#)

## 概要

この資料はコンピュータか Virtual Machine ( VM ) がイメージ変更されるか、または転用される  
ときエンドポイントのための識別永続性機能 on Cisco Advanced Malware Protection ( AMP ) が  
コンピュータ オブジェクト 固有の識別番号 ( UUID ) が再使用されるようにどのようにユニバー  
サルするかこと記述します。これはダッシュボードの重複したコンピュータ オブジェクトの作成  
を防ぎ、それらのコンピュータ オブジェクトの隣接するデータを維持します。これはまたエン  
ドポイント コネクタを維持し、データの継続を提供し、チェックでライセンス数の保存を助けます。

## 前提条件

### 要件

Cisco はこののナレッジがトピックあることを推奨します:

- Cisco AMP for Endpoints ダッシュボードへのアクセス
- 最初にコネクタを配置する前に設定識別永続性
- 識別永続性はウィンドウズオペレーティングシステム ( OS ) だけでサポートされます

注: 識別永続性機能は Cisco Technical Assistance Center ( TAC ) と有効にする必要があります。

### 使用するコンポーネント

この資料に記載されている情報は基づいた on Cisco AMP for Endpoints ダッシュボードです。

本書の情報は、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、初期 ( デフォルト ) 設定の状態から起動しています。対象の  
ネットワークが実稼働中である場合には、どのような作業についても、その潜在的な影響につい  
て確実に理解しておく必要があります。

# 作業の流れ

識別永続性オプションはこれが有効のときこれらの作業の流れを使用します:

1. 識別永続性オプションはポリシーで設定されます。
2. AMP for Endpoints インストーラはダッシュボードから生成され、新しいコンピュータが VM で配置されます。
3. 新しいコンピュータ オブジェクトは UUID および識別永続性フラグで作成されます。

## • 登録 チェック

コネクタ サービスが開始するとき、クラウド登録 チェックは実行された。登録 チェックは現在のマシンのような、ホスト名および MAC アドレスの情報を評価します。それはまた新しい UUID が生成される必要があったかどうか確認するためにクラウドに対してポリシーで設定する識別永続性を評価します。

## • 登録 基準

コンピュータ オブジェクトに使用される識別永続性設定に対応する非表示フラグが設定があります。固有の情報と共にこのフラグが、(ホスト名か MAC アドレス)条件を満たすあらゆるマシンに既存の UUID を提供するのに使用されています。マシンのフラグおよび固有の情報があらゆる既存のコンピュータ オブジェクトと一致する場合、新しい UUID およびオブジェクトはマシンのために生成されます。

注: ホスト名を使用するとき、完全修飾ドメイン名 (FQDN) は使用されます。テストと名付けられるマシンおよび `test.domain.com` と名付けられる別のマシンがある場合一致するし、UUID は再使用されません。

## • コンピュータを移動する方法

異なる識別永続性設定を持つグループ間のコンピュータの移動は重複を作成します。各識別永続性設定と関連付けられるこれは非表示 フラグが原因です。設定が一致するとき、重複は生成されます。グループは両方ともポリシー設定を渡ってを使用するとき同じポリシーを適用してもらわなければなりません。設定が同じならば、ポリシーが異なっていれば、重複は作成されます。

注: クローンとして作りたいと思うかまたは Cisco AMP for Endpoints のコンピュータがインストールしたイメージ、[この資料](#)を読んで下さい。

## • MAC アドレス選択

マシンは多重 MAC アドレスがあるかもしれませんが、手動でコネクタ 登録の間に MAC アドレス選択プロセスに影響を及ぼすことはできません。、他では使用すればホスト名をマシンに 1 MAC アドレスがあるただことを保証できるときだけ MAC アドレス設定を使用して下さい。

## • デフォルト グループ

識別永続性はまたデフォルト グループに適用されるポリシーのために設定する必要があります。ポリシーかグループがアクティブなマシンによって削除されれば、マシンはデフォルト グループに登録 チェックが次の時間実行されたとき置かれます。識別永続性がデフォルト グループのために設定されない場合、重複オブジェクトは生成されます。

注: 場合によっては、クローンとして作られた VM はからクローンとして作られたグループよりもむしろデフォルト グループに置かれるかもしれません。これが発生する場合、

FireAMP コンソールの正しいグループに VM を移動して下さい。

## 設定

識別永続性のコネクタを配置するためにステップにここに従って下さい:

ステップ 1.設定 するポリシーに望ましい識別永続性を適用して下さい:

- **管理 > ポリシー**にナビゲートして下さい
- 望ましいポリシーを選択して下さい。 『Edit』 をクリックして下さい
- **General タブ**にナビゲートして下さい。 それは、デフォルトで選択されます
- **コネクタ識別永続性**を選択して下さい。 **識別同期**はイメージに示すように現われず廃棄します。

# ← Edit Policy: Test

Policy for **FireAMP Windows**

Name	<input type="text" value="Test"/>
Simple Custom Detections	<input type="text" value="None"/>
Advanced Custom Detections	<input type="text" value="None"/>
Application Blocking	<input type="text" value="None"/>
Application Whitelist	<input type="text" value="None"/>
Exclusion Set	<input type="text" value="None"/>
IP Blacklists & Whitelists	<input type="button" value="Edit"/>
Description	<div style="border: 1px solid #ccc; height: 100px;"></div>

General | File | Network

**Administrative Features**

**Connector Identity Persistence**

Identity Synchronization	<input type="text" value="None"/>
--------------------------	-----------------------------------

Client User Interface

Proxy Settings

Product Updates

注: エンドポイントのインストールが重複したオブジェクトを各マシンのために生成します  
場合があった後機能の enablement。

環境のための推奨である**識別同期オプション**を選択して下さい。次のオプションを使用できます。

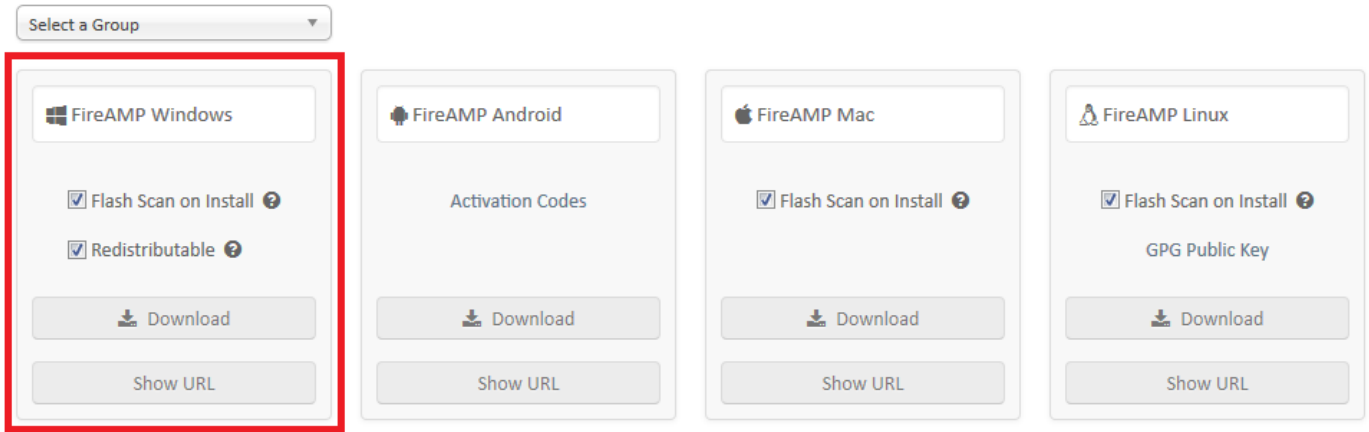
- **None** : 機能は有効になりません。コネクタ UUIDs はあらゆる状況のもとで新しいコネクタによってインストールします同期されません。各々の新しいインストールは新しいマシンオブジェクトを生成します。
- **ビジネスを渡る MAC アドレスによって**: 新しいコネクタは同じ MAC アドレスがどれも以外値に設定される識別同期がないビジネスのすべてのポリシーを渡って同期するためにある最新コネクタを探します。選択されたとき、マシン オブジェクトは全体のアカウントを渡るその MAC アドレスを使用するあらゆるマシンによって同期するために作成され、フラグを付けられます。
- **ポリシーを渡る MAC アドレスによって**: 新しいコネクタは同じ MAC アドレスが同じポリシーの内だと同期するためにある最新コネクタを探します。選択されたとき、マシン オブジェクトはその MAC アドレスを使用する割り当てられます特定のポリシーに対して登録されていて作成され、フラグを付けられ、あらゆるマシンによって同期するために。
- **ビジネスを渡るホスト名によって**: 新しいコネクタは同じホスト名をどれも以外値に設定される識別同期がないビジネスのすべてのポリシーを渡ってと同期するために備えている最新コネクタを探します。選択されたとき、マシン オブジェクトは全体のアカウントを渡るそのホスト名を使用するあらゆるマシンによって同期するために作成され、フラグを付けられます。注: 識別永続性を使用するために選択する場合 Cisco は**ビジネスを渡るホスト名**によって使用することを推奨します。マシンは 1 ホスト名を備えていたり、複数の MAC アドレスを持つ場合があります。ビジネスを渡る設定はオブジェクトをポリシーごとによりもむしろグローバルに利用できるようにすると同時に設定の複雑な状況を簡素化できます。
- **ポリシーを渡るホスト名によって**: 新しいコネクタは同じホスト名を同じポリシーの内だと同期するために備えている最新コネクタを探します。選択されたとき、マシン オブジェクトは作成され、あらゆるマシンに同期するためにフラグを付けられ、そのホスト名を使用する特定のポリシーに登録されています。

ステップ 2.イメージに示すようにクラウド ダッシュボードからインストール パッケージをダウンロードして下さい:

- **管理 > ダウンロード コネクタ**にナビゲートして下さい
- 望ましいグループ名およびオプションを選択して下さい
- 『Download』 をクリックして下さい
- サードパーティ配備ソフトウェアのために **Redistributable**、か**オフ・ライン インストール**を使用して下さい

注: Cisco はサードパーティ配備ソフトウェアを使用するパッケージまたはインストールの作成をサポートしません。

## Download Connector



ステップ 3.組織のマシンにコネクタを配置して下さい。

## 確認

このセクションでは、設定が正常に機能していることを確認します。

識別永続性作業が、次の手順に従うかどうか確認するため:

1. コンピュータ オブジェクトを生成するために識別同期のためにフラグを付けられるコネクタをインストールして下さい。
2. オブジェクトが作成された後、インストール ディレクトリ C:\Program Files\Sourcefire\fireAMP\local.xml の local.xml ファイルから <uuid> のメモを作して下さい。これと同じような行を見て下さい:  
`<uuid>1234567890-abcd-efgh-ijkl-mnopqrst</uuid>`
3. その後、コネクタをアンインストールして下さい。インストール パスから取除かれるすべてのファイルを持つために『No』を選択して下さい。
4. PC をリブートし、先にと同じパッケージとの AMP for Endpoints を再インストールして下さい。
5. local.xml ファイルを第一歩によって再度チェックし、オリジナル local.xmlfile からの UUID と一致するようにして下さい。

## トラブルシューティング

このセクションでは、設定のトラブルシューティングに役立つ情報を提供します。

- インストール パッケージおよび識別永続性設定が一貫していることを確認して下さい。
- 識別永続性配置後を有効にし、有効になる識別永続性なしでコネクタをインストールするためにより古いパッケージを使用すればコネクタは登録する生成し、現在の設定とのポリシーをアップデートしますと同時に重複を。
- UUID を共有するマシンがようである場合固有の情報を共有しない仮想化された環境内の MAC アドレスのようように、して下さい。

## 関連情報

- [Advanced Malware Protection エンドポイント](#)
- [テクニカル サポートとドキュメント - Cisco Systems](#)