

AMP for Endpointsポータルでの簡易カスタム検出リストの設定

内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[ワークフロー](#)

[コンフィギュレーション](#)

[確認](#)

[トラブルシューティング](#)

概要

このドキュメントでは、Advanced Malware Protection(AMP)for Endpointsコネクタをインストールしたデバイスで許可されるファイルを防止するために、特定のファイルを検出、ブロック、および検疫するための簡易カスタム検出リストを作成する手順について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- AMPポータルへのアクセス
- 管理者権限を持つアカウント
- ファイルサイズは20 MB以下

使用するコンポーネント

このドキュメントの情報は、Cisco AMP for Endpointsコンソールバージョン5.4.20190709に基づくものです。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。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。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

ワークフロー

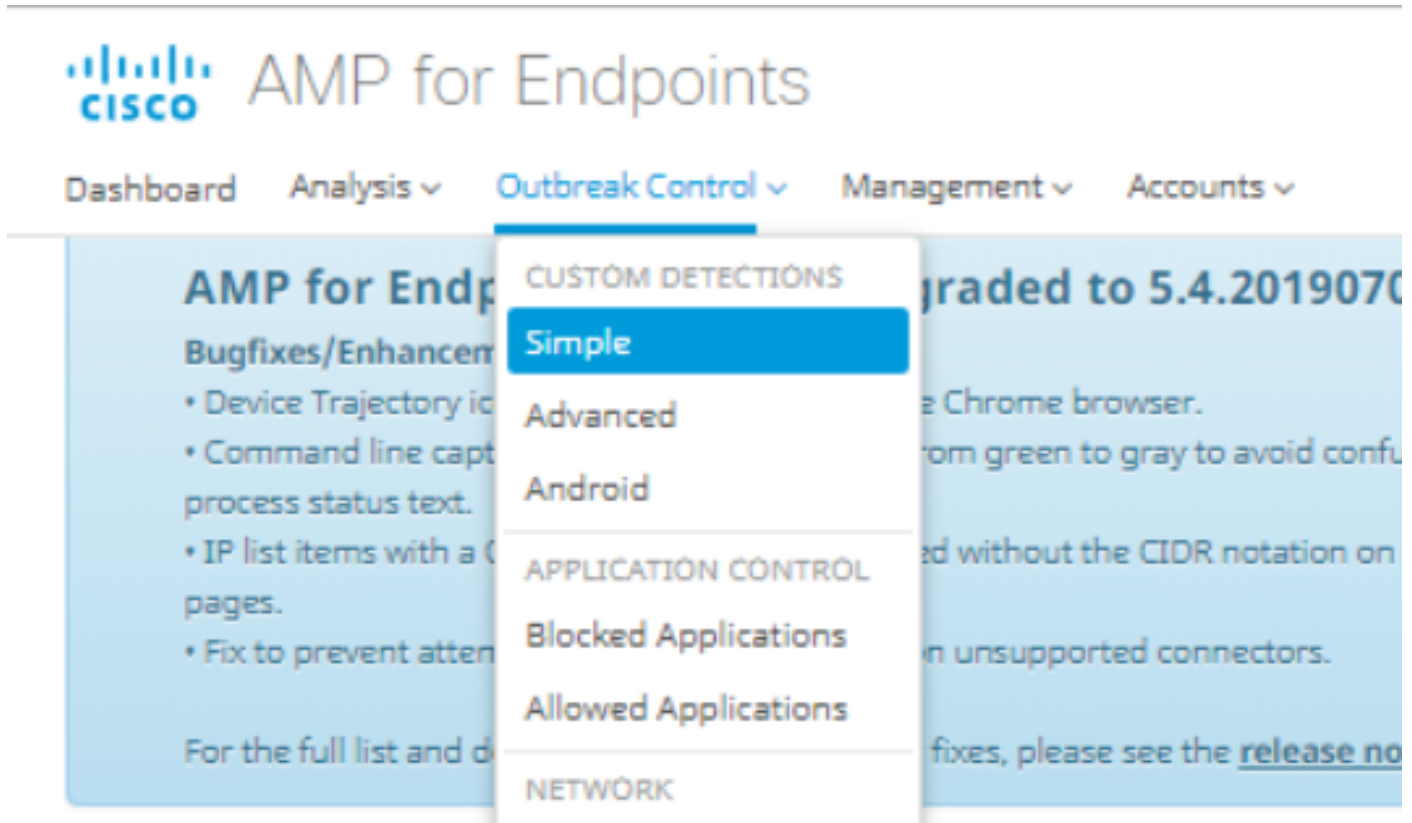
[Simple Custom Detection]リストオプションでは、次のワークフローを使用します。

- AMPポータルから作成された簡易カスタム検出リスト。
- 以前に作成したポリシーに適用された簡易カスタム検出リスト。
- デバイスにインストールされ、ポリシーに適用されたAMPコネクタ。

コンフィギュレーション

簡易カスタム検出リストを作成するには、次の手順を実行します。

ステップ1：図に示すように、AMPポータルで[Outbreak Control] > [Simple]オプションに移動します。



ステップ2:[Custom Detections - Simple]オプションで、[Create]ボタンをクリックして新しいリストを追加し、名前を選択して[Simple Custom Detection]リストを識別し、図に示すように保存します。

Custom Detections - Simple

ステップ3：リストが作成されたら、[Edit]ボタンをクリックして、ブロックするファイルのリストを追加します（図を参照）。

Custom_list_1

0 files

Created by Yeraldin Sanchez Mendoza • 2019-07-14 18:33:13 UTC

Not associated with any policy or group

[View Changes](#)

[Edit](#)

[Delete](#)

ステップ4:[Add SHA-256]オプションで、ブロックする特定のファイルから以前に収集したSHA-256コードを貼り付けます (図を参照)。

Custom_list_1 [Update Name](#)

[Add SHA-256](#) [Upload File](#) [Upload Set of SHA-256s](#)

Add a file by entering the SHA-256 of that file

SHA-256

Note

[Add](#)

Files included

You have not added any files to this list

ステップ5:[Upload File]オプションで、ブロックする特定のファイルを参照します。ファイルがアップロードされると、このファイルのSHA-256がリストに追加されます (図を参照)。

[Add SHA-256](#) [Upload File](#) [Upload Set of SHA-256s](#)

Upload a file to be added to your list (20 MB limit)

File [Browse](#)

Note

[Upload](#)

Files included

ステップ6:[Upload Set of SHA-256]オプションを使用すると、図に示すように、以前に取得した複数のSHA-256コードのリストを含むファイルを追加できます。

SHA256_list.txt - Notepad

File Edit Format View Help

```
85B5F70F84A10FC22271D32B82393EF28CAA55A534F8C08EE3A7DC76139A4DE2  
CEAFF4CD2FDE8B313C52479984E95C0E66A7727313B27516D8F3C70E9F74D71D  
89D599BB4BB64AF353329C1A7D32F1E3FF8C5E0B22D27A4AFEE6A1C3697A0D2A
```

The screenshot shows the 'Upload Set of SHA-256s' interface in the AMP for Endpoints console. At the top, there is a text input field containing 'Custom_list_1' and an 'Update Name' button. Below this are three tabs: 'Add SHA-256', 'Upload File', and 'Upload Set of SHA-256s', with the third tab selected. The main area contains the instruction 'Upload a file containing a set of SHA-256s'. There is a 'File' input field with 'SHA256_list.txt' and a 'Browse' button. Below that is a 'Note' input field with the text 'This is the SHA256 list to block'. At the bottom of this section is an 'Upload' button with an upward arrow icon. Below the upload section is a 'Files included' section.

ステップ7:[Simple Custom Detection]リストが生成されたら、[Management] > [Policies]に移動し、図に示すように、以前に作成したリストを適用するポリシーを選択します。

The screenshot shows the navigation menu of the AMP for Endpoints console. The menu items are: Dashboard, Analysis, Outbreak Control, Management, and Accounts. The 'Management' menu is expanded, showing a list of options: Quick Start, Computers, Groups, Policies, Exclusions, Download Connector, Deploy Clarity for iOS, and Deployment Summary. The 'Policies' option is highlighted with a grey background. On the left side of the screenshot, there is a blue sidebar with the text 'AMP for Endpoints Console' and 'Bugfixes/Enhancement' followed by a list of updates.

WIN POLICY LEISANCH			
Modes and Engines	Exclusions	Proxy	Groups
Files Quarantine Network Disabled Malicious Activity Prot... Disabled System Process Protec... Disabled	leisanch2Excl Microsoft Windows Default Windows leisanch Policy	Not Configured	leisanch_group2 1 leisanch_RE-renamed_1 1
Outbreak Control			
Custom Detections - Simple	Custom Detections - Advanced	Application Control	Network
Not Configured	Not Configured	leisanch_blocking2 Blocked	Not Configured
View Changes Modified 2019-07-15 20:04:21 UTC Serial Number 12625		Download XML	Duplicate Edit Delete

ステップ8:[Edit]ボタンをクリックし、[Outbreak Control] > [Custom Detections - Simple]に移動し、ドロップダウンメニューで以前に生成したリストを選択して、変更を保存します(図を参照)。

< Edit Policy

Windows

Name WIN POLICY LEISANCH

Description

Modes and Engines	Custom Detections - Simple	Custom_list_1
Exclusions 3 exclusion sets	Custom Detections - Advanced	None
Proxy	Application Control - Allowed	None
Outbreak Control	Application Control - Blocked	leisanch_blocking2
Product Updates	Network - IP Block & Allow Lists	Clear Select Lists
Advanced Settings	None	

Cancel Save

すべての手順が実行され、コネクタが最後のポリシー変更と同期されると、簡易カスタム検出が有効になります。

確認

現在、この設定に使用できる確認手順はありません。

トラブルシューティング

現在、この設定に関する特定のトラブルシューティング情報はありません。

警告：ファイルが簡易カスタム検出リストに追加された場合、検出が有効になるまでにキャッシュ時間が経過する必要があります。

注：簡易カスタム検出を追加すると、キャッシュされます。ファイルがキャッシュされる時間は、次のリストに示すように、その性質によって異なります。

- ・ ファイルのクリーニング：7 日
- ・ 不明なファイル：1 時間
- ・ 悪意のあるファイル：1 時間