

在面向終端的AMP門戶上配置簡單自定義檢測清單

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[工作流程](#)

[組態](#)

[驗證](#)

[疑難排解](#)

簡介

本文檔介紹建立簡單自定義檢測清單以檢測、阻止和隔離特定檔案的步驟，以防止在安裝了面向終端的高級惡意軟體防護(AMP)聯結器的裝置上允許這些檔案。

必要條件

需求

思科建議您瞭解以下主題：

- 訪問AMP門戶
- 具有管理員許可權的帳戶
- 檔案大小不超過20 MB

採用元件

本檔案中的資訊是根據思科終端進階惡意軟體防護主控台版本5.4.20190709。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

工作流程

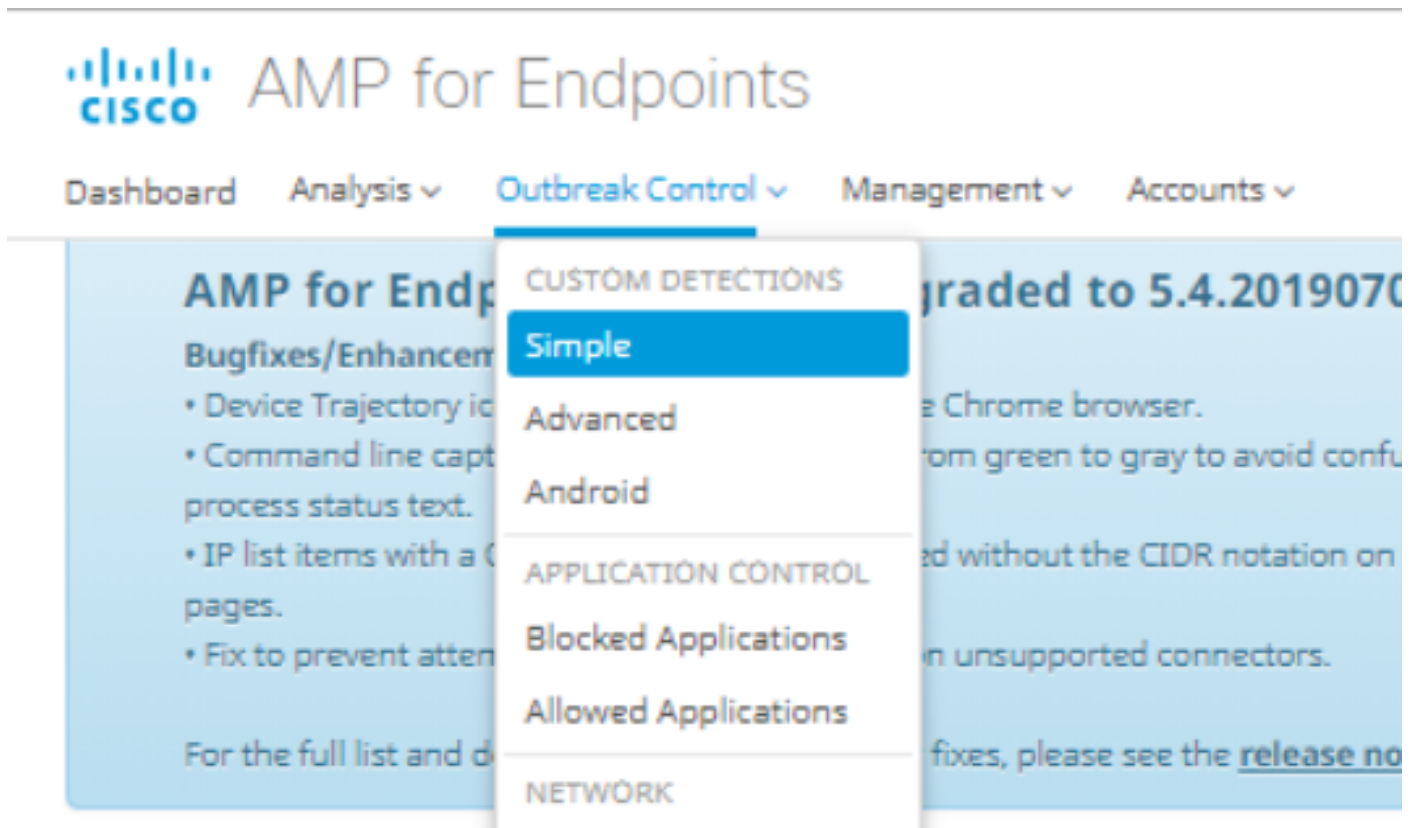
簡單自定義檢測清單選項使用以下工作流程：

- 從AMP門戶建立的簡單自定義檢測清單。
- 在先前建立的策略中應用的簡單自定義檢測清單。
- AMP聯結器安裝在裝置上並應用於策略。

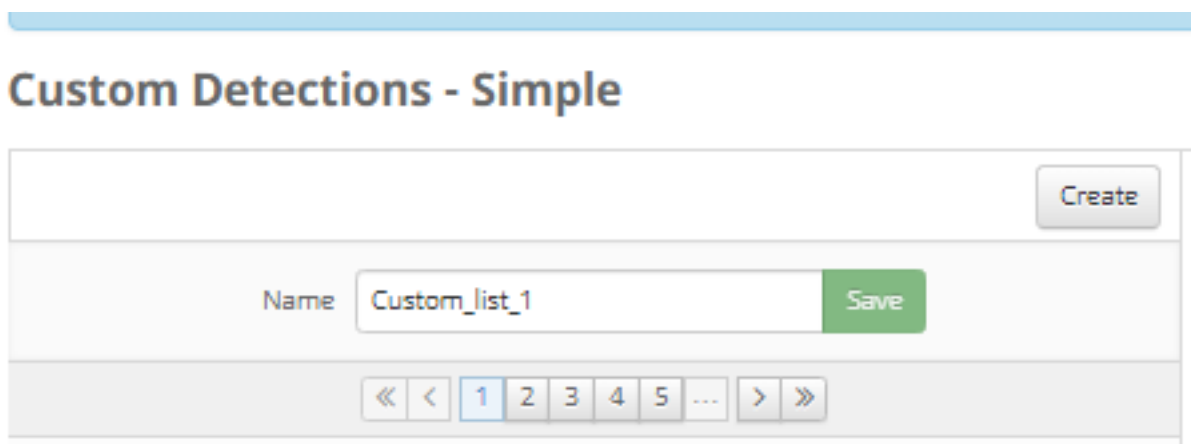
組態

要建立簡單自定義檢測清單，請執行以下步驟：

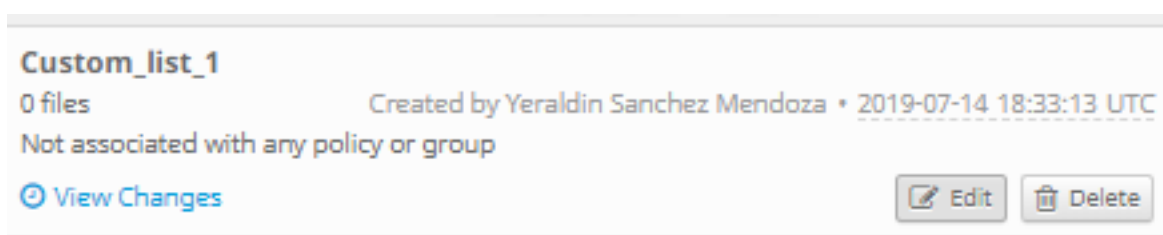
步驟1. 在AMP門戶上，導覽至**Outbreak Control > Simple**選項，如下圖所示。



步驟2. 在Custom Detections - Simple選項上，按一下**Create**按鈕新增新清單，選擇一個名稱以標識Simple Custom Detection清單並儲存它，如下圖所示。



步驟3. 建立清單後，按一下**Edit**按鈕以新增要封鎖的檔案清單，如下圖所示。



步驟4.在Add SHA-256 (新增SHA-256) 選項上，貼上之前從要阻止的特定檔案中收集的SHA-256代碼，如圖所示。

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

步驟5.在「Upload File」選項上，瀏覽要阻止的特定檔案，一旦檔案上傳，就會將此檔案的SHA-256新增到清單中，如下圖所示。

[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

步驟6. Upload Set of SHA-256s選項允許新增包含之前獲取的多個SHA-256代碼清單的檔案，如圖所示。

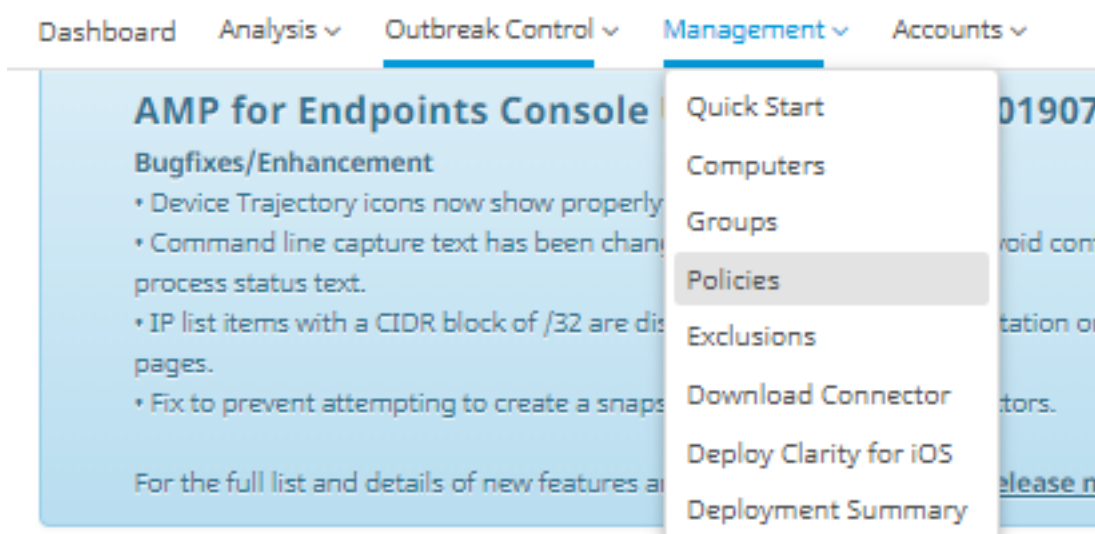
SHA256_list.txt - Notepad

File Edit Format View Help

```
85B5F70F84A10FC22271D32B82393EF28CAA55A534F8C08EE3A7DC76139A4DE2  
CEAFF4CD2FDE8B313C52479984E95C0E66A7727313B27516D8F3C70E9F74D71D  
89D599BB4BB64AF353329C1A7D32F1E3FF8C5E0B22D27A4AFEE6A1C3697A0D2A
```

The screenshot shows a web interface for uploading a custom list of SHA-256 hashes. At the top, there is a text input field containing 'Custom_list_1' and an 'Update Name' button. Below this are three buttons: 'Add SHA-256', 'Upload File', and 'Upload Set of SHA-256s'. The 'Upload Set of SHA-256s' button is selected. Underneath, there is a section titled 'Upload a file containing a set of SHA-256s'. It includes a 'File' input field with 'SHA256_list.txt' and a 'Browse' button. Below that is a 'Note' input field containing 'This is the SHA256 list to block'. At the bottom of this section is an 'Upload' button with a downward arrow icon. Below the upload section is a heading 'Files included'.

步驟7.生成簡單自定義檢測清單後，導航到**管理>策略**，然後選擇要在其中應用先前建立的清單的策略，如圖所示。



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

步驟8. 按一下**Edit**按鈕並導航到**Outbreak Control > Custom Detections - Simple**，選擇以前在下拉選單上生成的清單並儲存更改，如下圖所示。

< 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

執行完所有步驟，並將連結器與上次策略更改同步後，簡單自定義檢測將生效。

驗證

目前沒有適用於此組態的驗證程序。

疑難排解

目前尚無適用於此組態的具體疑難排解資訊。

警告：如果將檔案新增到簡單自定義檢測清單，則在檢測生效之前，快取時間必須過期。

附註：新增簡單自定義檢測時，該檢測將被快取。檔案快取的時間長度取決於其性質，如以下清單所示：

- 清理檔案：7天
- 未知檔案：1小時
- 惡意檔案：1小時