

Configure una lista de detección personalizada sencilla en el portal de AMP para terminales

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Flujo de trabajo](#)

[Configuración](#)

[Verificación](#)

[Troubleshoot](#)

Introducción

Este documento describe los pasos para crear una lista de detección personalizada simple para detectar, bloquear y poner en cuarentena archivos específicos para evitar que se permita el acceso a los archivos en dispositivos que han instalado los conectores de protección frente a malware avanzado (AMP) para terminales.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Acceso al portal de AMP
- Cuenta con privilegios de administrador
- Tamaño del archivo no superior a 20 MB

Componentes Utilizados

La información de este documento se basa en la versión 5.4.20190709 de la consola de Cisco AMP para terminales.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Flujo de trabajo

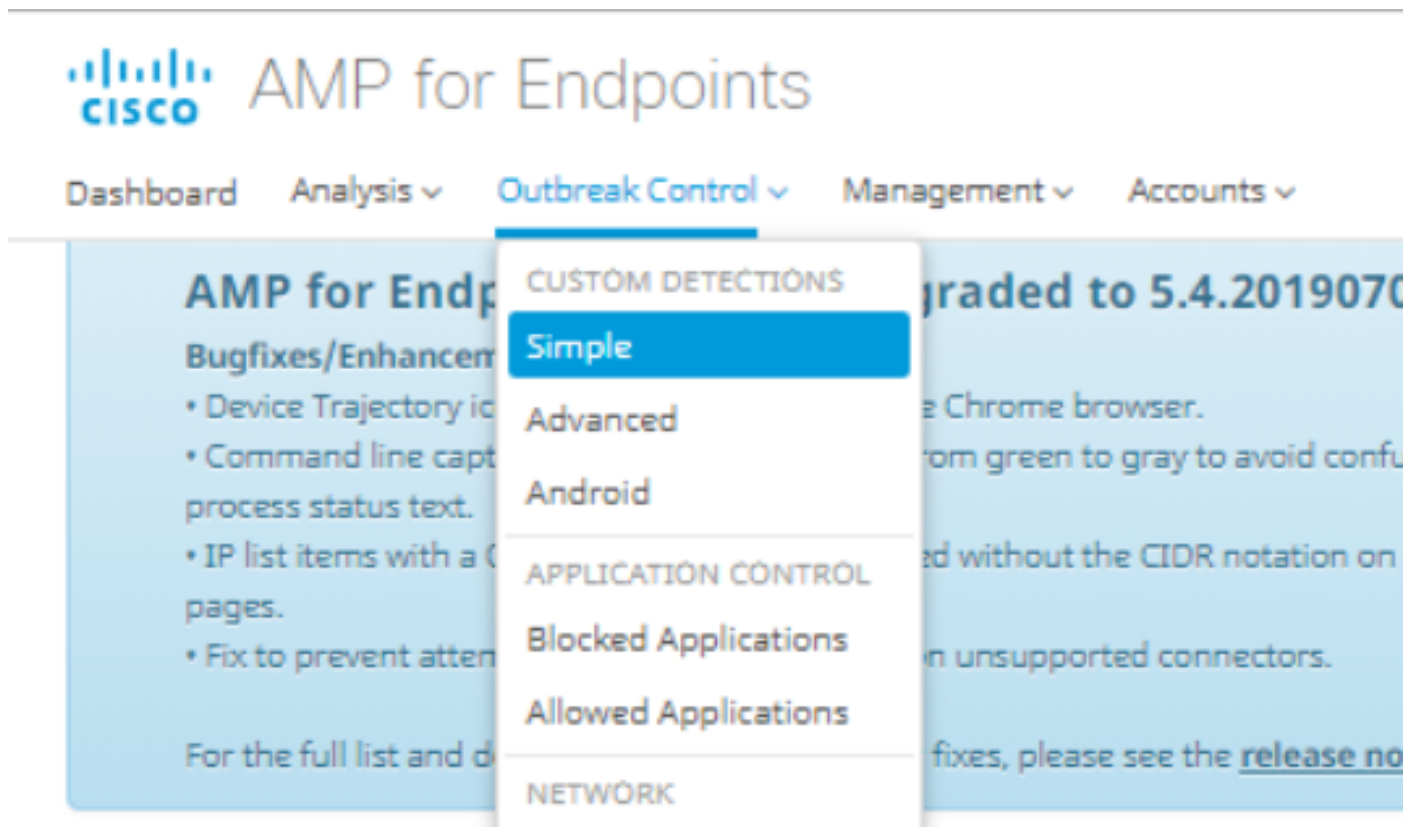
La opción de lista Simple Custom Detection utiliza este flujo de trabajo:

- La lista Simple Custom Detection creada desde el portal de AMP.
- Una lista de detección personalizada simple aplicada en una política creada anteriormente.
- El conector de AMP instalado en el dispositivo y aplicado en la política.

Configuración

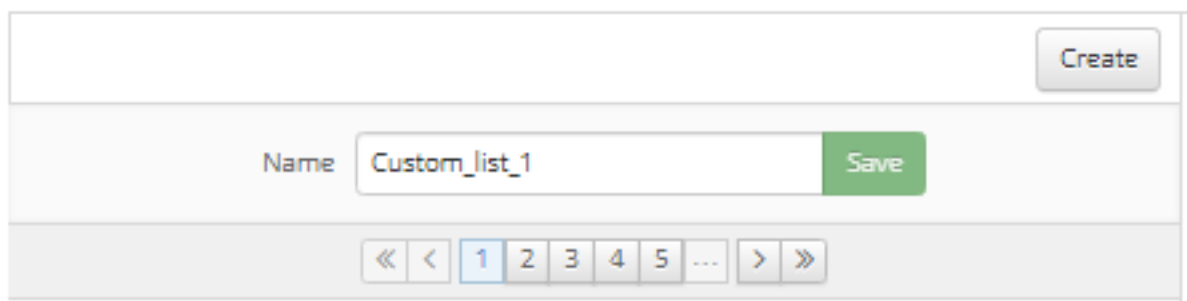
Para crear una lista de detección personalizada simple, siga estos pasos:

Paso 1. En el portal de AMP, vaya a la opción **Control de brotes > Simple**, como se muestra en la imagen.



Paso 2. En la opción Detección personalizada - Simple, haga clic en el botón **Crear** para agregar una nueva lista, elija un nombre para identificar la lista Detección personalizada simple y guárdelo, como se muestra en la imagen.

Custom Detections - Simple

The image shows the 'Custom Detections - Simple' form. At the top right, there is a 'Create' button. Below it, there is a 'Name' field with the text 'Custom_list_1' and a green 'Save' button. At the bottom, there is a pagination control with buttons for '<<', '<', '1', '2', '3', '4', '5', '...', '>', and '>>'. The '1' button is highlighted.

Paso 3. Una vez creada la lista, haga clic en el botón **Edit** para agregar la lista de los archivos que desea bloquear, como se muestra en la imagen.

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](#)

Paso 4. En la opción Add SHA-256 (Agregar SHA-256), pegue el código SHA-256 recolectado anteriormente del archivo específico que desea bloquear, como se muestra en la imagen.

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

Paso 5. En la opción Cargar archivo, busque el archivo específico que desea bloquear, una vez que se haya cargado el archivo, el SHA-256 de este archivo se agregará a la lista, como se muestra en la imagen.

[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

Paso 6. La opción Upload Set of SHA-256s permite agregar un archivo con una lista de varios códigos SHA-256 adquiridos previamente, como se muestra en las imágenes.

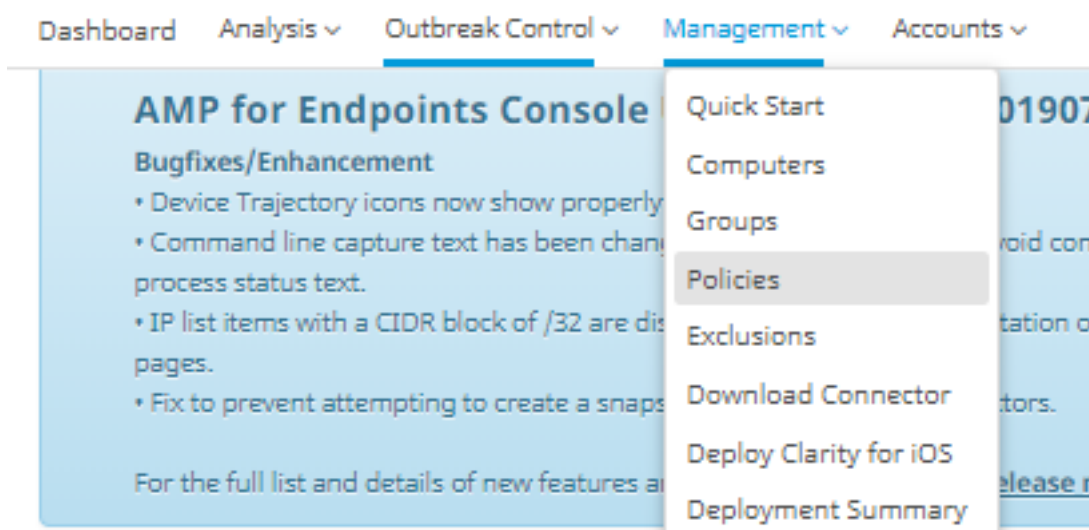
SHA256_list.txt - Notepad

File Edit Format View Help

```
85B5F70F84A10FC22271D32B82393EF28CAA55A534F8C08EE3A7DC76139A4DE2  
CEAFF4CD2FDE8B313C52479984E95C0E66A7727313B27516D8F3C70E9F74D71D  
89D599BB4BB64AF353329C1A7D32F1E3FF8C5E0B22D27A4AFEE6A1C3697A0D2A
```

The screenshot shows a web interface for uploading a custom detection list. 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 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 heading 'Files included'.

Paso 7. Una vez generada la lista Simple Custom Detection, navegue hasta **Management > Policies** y elija la política donde desea aplicar la lista previamente creada, como se muestra en las imágenes.



Modes and Engines		Exclusions	Proxy	Groups
Files	Quarantine	leisanch2Excl	Not Configured	leisanch_group2 1
Network	Disabled	Microsoft Windows Default		leisanch_RE-renamed_1 1
Malicious Activity Prot...	Disabled	Windows leisanch Policy		
System Process Protec...	Disabled			
Outbreak Control				
Custom Detections - Simple		Custom Detections - Advanced		Application Control
Not Configured		Not Configured		leisanch_blocking2 Blocked
				Network
				Not Configured

[View Changes](#) Modified 2019-07-15 20:04:21 UTC Serial Number 12625
 [Download XML](#)
[Duplicate](#)
[Edit](#)
[Delete](#)

Paso 8. Haga clic en el botón **Editar** y navegue hasta **Control de brotes > Detección personalizada - Simple**, seleccione la lista previamente generada en el menú desplegable y guarde los cambios, como se muestra en la imagen.

< Edit Policy

Windows

Name WIN POLICY LEISANCH

Description

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

Una vez que se realizan todos los pasos y los conectores se sincronizan con los últimos cambios de política, entra en vigor la detección personalizada simple.

Verificación

Actualmente, no hay un procedimiento de verificación disponible para esta configuración.

Troubleshoot

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.

Advertencia: Si se agrega un archivo a una lista de detección personalizada simple, el tiempo de caché debe caducar antes de que surta efecto la detección.

Nota: Cuando agrega una detección personalizada simple, está sujeto a almacenamiento en caché. El tiempo que un archivo se almacena en caché depende de su disposición, como se muestra en esta lista:

·Limpiar archivos: 7 días

Archivos · desconocidos: 1 hora

Archivos malintencionados ·: 1 hora