

Configurare un elenco di rilevamento personalizzato semplice nel portale AMP for Endpoints

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Flusso di lavoro](#)

[Configurazione](#)

[Verifica](#)

[Risoluzione dei problemi](#)

Introduzione

In questo documento viene descritto come creare un elenco di rilevamento personalizzato semplice per rilevare, bloccare e mettere in quarantena file specifici al fine di impedire che i file vengano autorizzati sui dispositivi che hanno installato i connettori Advanced Malware Protection (AMP) for Endpoints.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Accesso al portale AMP
- Account con privilegi di amministratore
- Dimensioni del file non superiori a 20 MB

Componenti usati

Il riferimento delle informazioni contenute in questo documento è la console Cisco AMP for Endpoints versione 5.4.20190709.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Flusso di lavoro

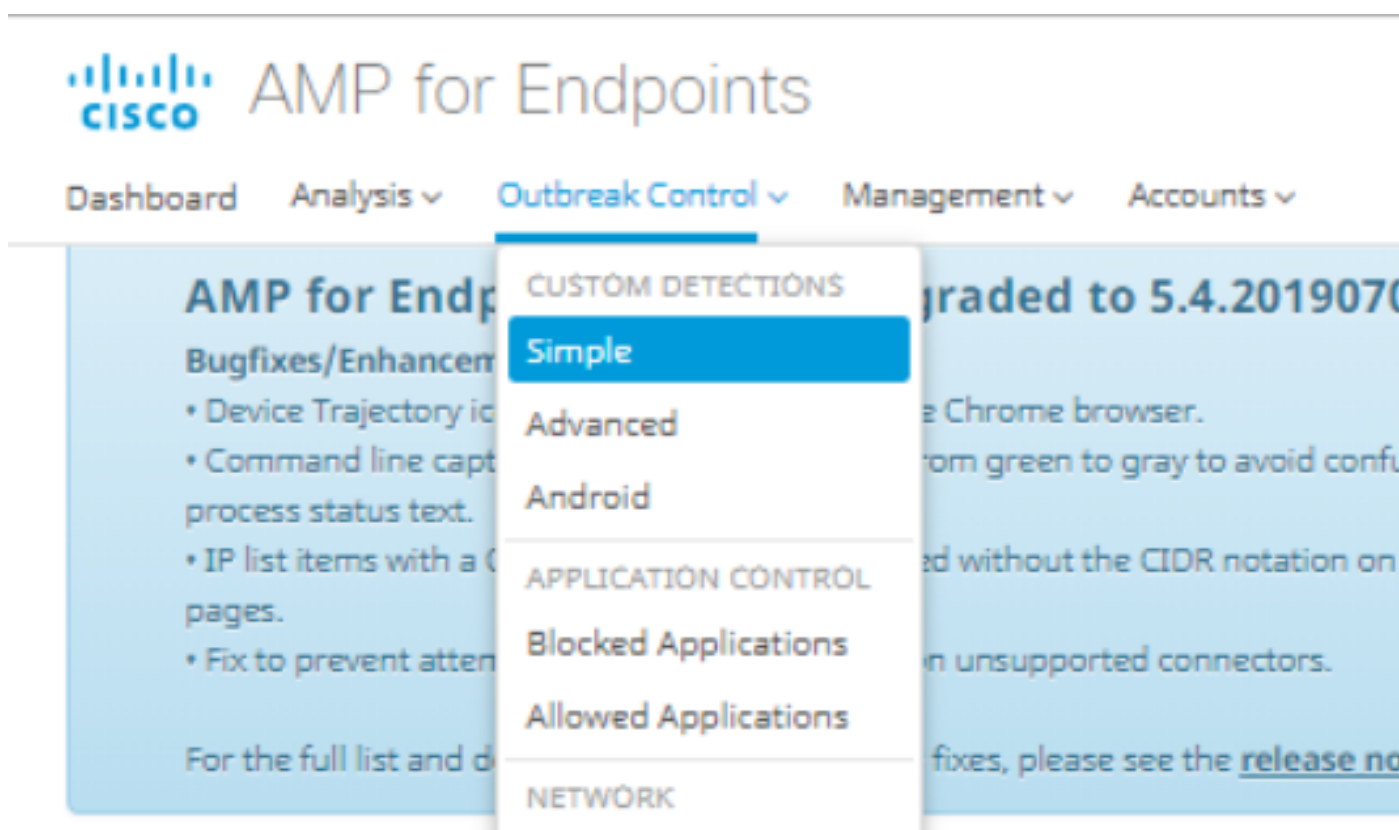
L'opzione Elenco rilevamento personalizzato semplice utilizza il flusso di lavoro seguente:

- Elenco di rilevamento personalizzato semplice creato dal portale AMP.
- Elenco di rilevamento personalizzato semplice applicato in un criterio creato in precedenza.
- Il connettore AMP installato nel dispositivo e applicato nel criterio.

Configurazione

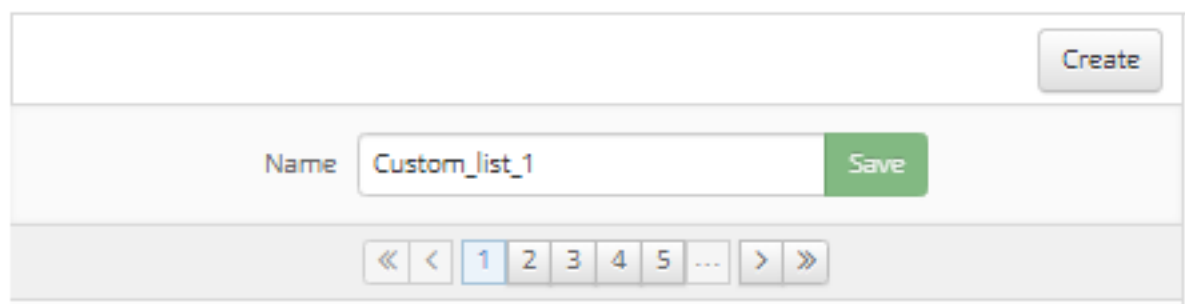
Per creare un elenco di rilevamento personalizzato semplice, eseguire la procedura seguente:

Passaggio 1. Sul portale AMP, selezionare **Controllo epidemie > Semplice**, come mostrato nell'immagine.

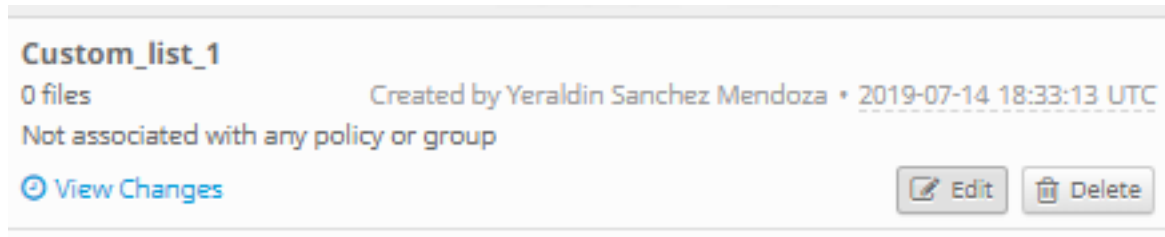


Passaggio 2. Nell'opzione Rilevamenti personalizzati - Semplici, fare clic su **Crea** pulsante per aggiungere un nuovo elenco, scegliere un nome per identificare l'elenco Rilevamento personalizzato semplice e salvarlo, come mostrato nell'immagine.

Custom Detections - Simple

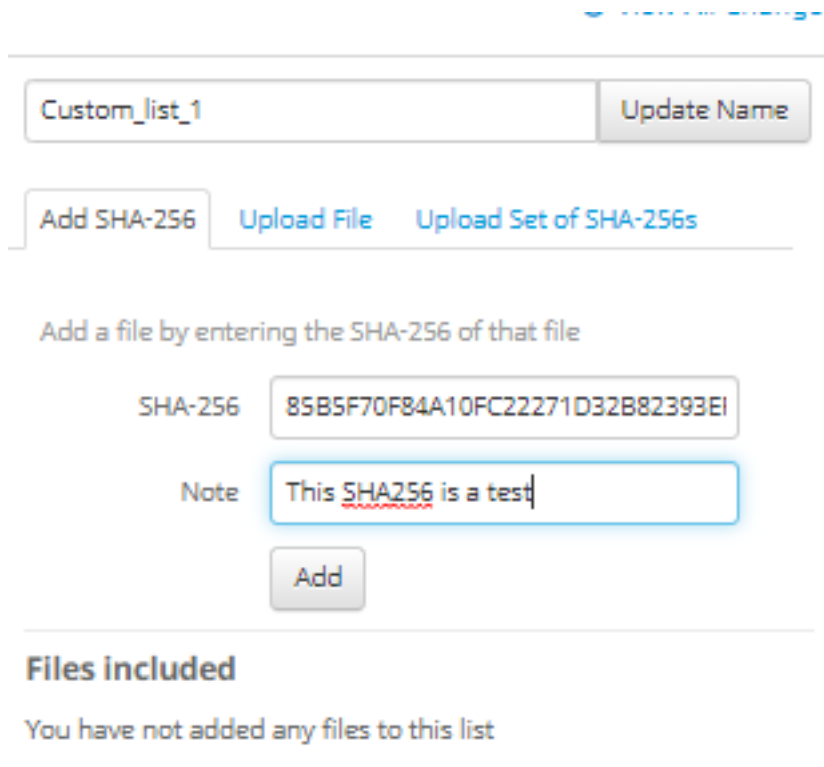
The image shows a screenshot of the 'Custom Detections - Simple' configuration page. At the top right, there is a 'Create' button. Below it, there is a 'Name' field containing the text 'Custom_list_1' and a green 'Save' button. At the bottom, there is a pagination control with a '1' button highlighted, indicating the current page.

Passaggio 3. Una volta creato l'elenco, fare clic sul pulsante **Edit** (Modifica) per aggiungere l'elenco dei file che si desidera bloccare, come mostrato nell'immagine.



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](#)

Passaggio 4. Nell'opzione Add SHA-256, incollare il codice SHA-256 precedentemente raccolto dal file specifico che si desidera bloccare, come mostrato nell'immagine.



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

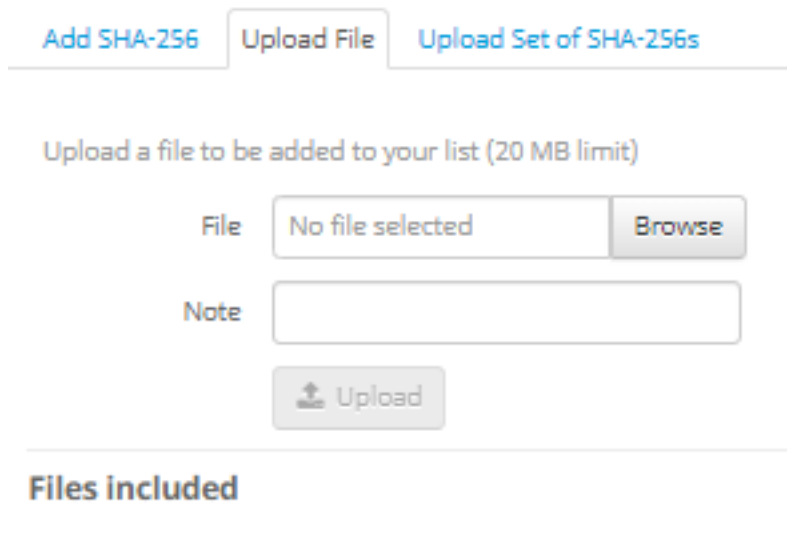
SHA-256

Note

[Add](#)

Files included
You have not added any files to this list

Passaggio 5. Nell'opzione Carica file, individuare il file specifico che si desidera bloccare, una volta caricato il file, l'SHA-256 di questo file viene aggiunto all'elenco, come mostrato nell'immagine.



[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

Passaggio 6. L'opzione Upload Set of SHA-256s consente di aggiungere un file con un elenco di più codici SHA-256 precedentemente acquisiti, come mostrato nelle immagini.

 SHA256_list.txt - Notepad

File Edit Format View Help

```
85B5F70F84A10FC22271D32B82393EF28CAA55A534F8C08EE3A7DC76139A4DE2  
CEAFF4CD2FDE8B313C52479984E95C0E66A7727313B27516D8F3C70E9F74D71D  
89D599BB4BB64AF353329C1A7D32F1E3FF8C5E0B22D27A4AFEE6A1C3697A0D2A
```

[Add SHA-256](#) [Upload File](#)

Upload a file containing a set of SHA-256s

File

Note

Passaggio 7. Una volta generato l'elenco Rilevamento custom semplice, passare a **Gestione > Criteri** e scegliere il criterio a cui applicare l'elenco creato in precedenza, come mostrato nelle immagini.

AMP for Endpoints Console

Bugfixes/Enhancement

- Device Trajectory icons now show properly
- Command line capture text has been changed to show process status text.
- IP list items with a CIDR block of /32 are displayed on the pages.
- Fix to prevent attempting to create a snapshot

For the full list and details of new features and bugfixes, see the release notes.

- Quick Start
- Computers
- Groups
- Policies**
- Exclusions
- Download Connector
- Deploy Clarity for iOS
- Deployment Summary

01907

avoid con

tation of

tors.

release n

WIN POLICY LEISANCH
2 2

Modes and Engines		Exclusions	Proxy	Groups
Files	Quarantine	leisanch2Excl Microsoft Windows Default Windows leisanch Policy	Not Configured	leisanch_group2 1
Network	Disabled			leisanch_RE-renamed_1 1
Malicious Activity Prot...	Disabled			
System Process Protec...	Disabled			
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 				

Passaggio 8. Fare clic sul pulsante **Modifica** e selezionare **Controllo epidemie > Rilevamenti personalizzati - Semplice**, selezionare l'elenco generato in precedenza dal menu a discesa e salvare le modifiche, come mostrato nell'immagine.

< 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

Dopo aver eseguito tutte le operazioni e aver sincronizzato i connettori con le ultime modifiche apportate ai criteri, viene attivato il rilevamento personalizzato semplice.

Verifica

Attualmente non è disponibile una procedura di verifica per questa configurazione.

Risoluzione dei problemi

Al momento non sono disponibili informazioni specifiche per la risoluzione dei problemi di questa configurazione.

Avviso: Se un file viene aggiunto a un elenco di rilevamento personalizzato semplice, il tempo di memorizzazione nella cache deve scadere prima che il rilevamento abbia effetto.

Nota: Quando si aggiunge un rilevamento personalizzato semplice, questo viene memorizzato nella cache. La durata della memorizzazione di un file nella cache dipende dalla relativa disposizione, come illustrato nell'elenco seguente:

- Pulizia dei file: 7 giorni

- File sconosciuti: 1 ora
- File dannosi: 1 ora