

Konfigurieren einer einfachen benutzerdefinierten Erkennungsliste im AMP für Endgeräte-Portal

Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Workflow](#)

[Konfiguration](#)

[Überprüfen](#)

[Fehlerbehebung](#)

Einführung

In diesem Dokument werden die Schritte zum Erstellen einer Liste einfacher benutzerdefinierter Erkennungsoptionen beschrieben, um bestimmte Dateien zu erkennen, zu blockieren und zu isolieren, damit die Dateien auf Geräten zugelassen werden, auf denen die AMP-Connectors (Advanced Malware Protection) für Endpoints installiert sind.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Zugriff auf das AMP-Portal
- Konto mit Administratorberechtigungen
- Dateigröße nicht mehr als 20 MB

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf Cisco AMP für Endgeräte Konsolenversion 5.4.20190709.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Workflow

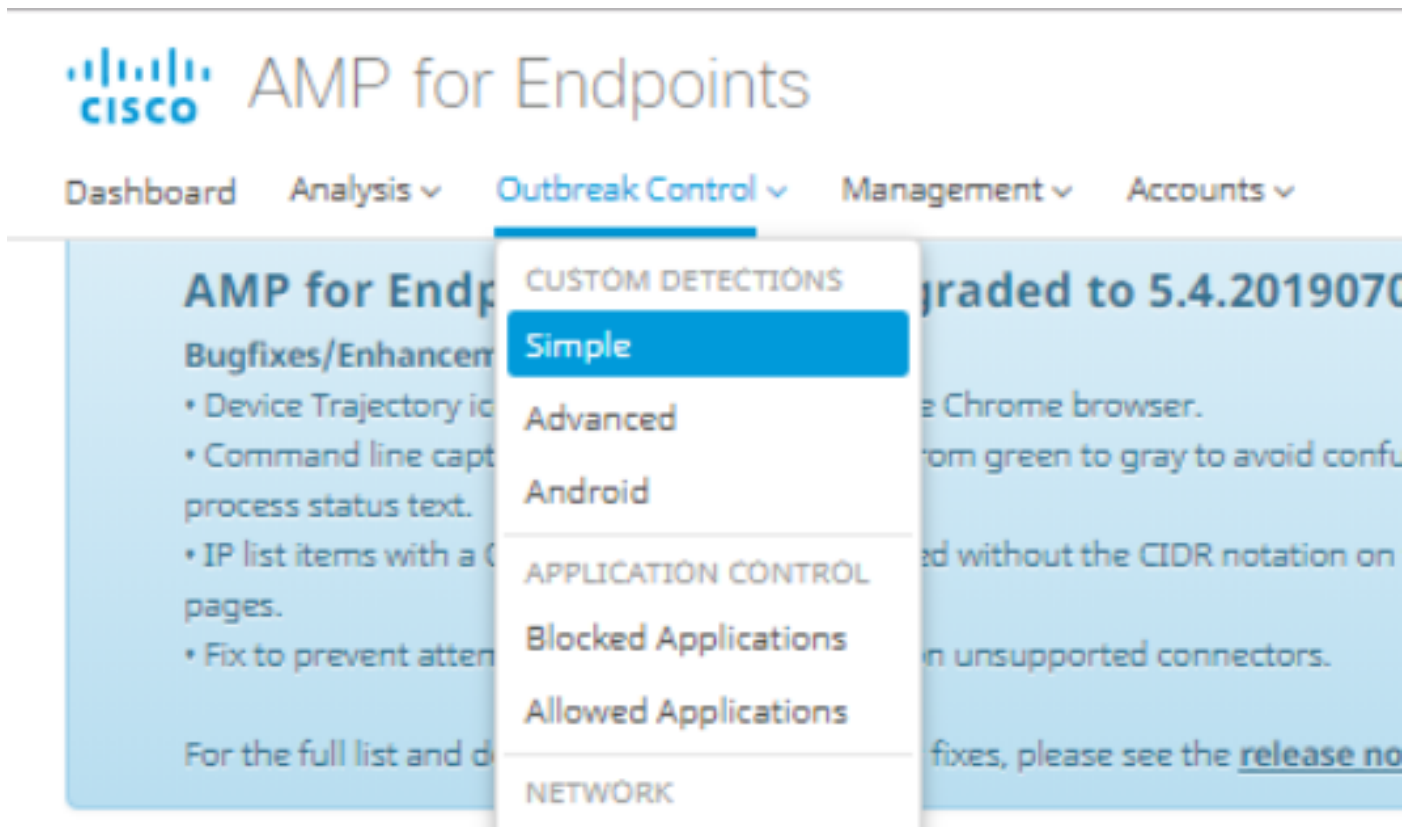
Die Option für die Liste einfacher benutzerdefinierter Erkennung verwendet diesen Workflow:

- Die Liste der einfachen benutzerdefinierten Erkennung, die über das AMP-Portal erstellt wurde.
- Eine Liste einfacher benutzerdefinierter Erkennungen, die in einer zuvor erstellten Richtlinie angewendet wurde.
- Der auf dem Gerät installierte und in der Richtlinie angewendete AMP-Anschluss.

Konfiguration

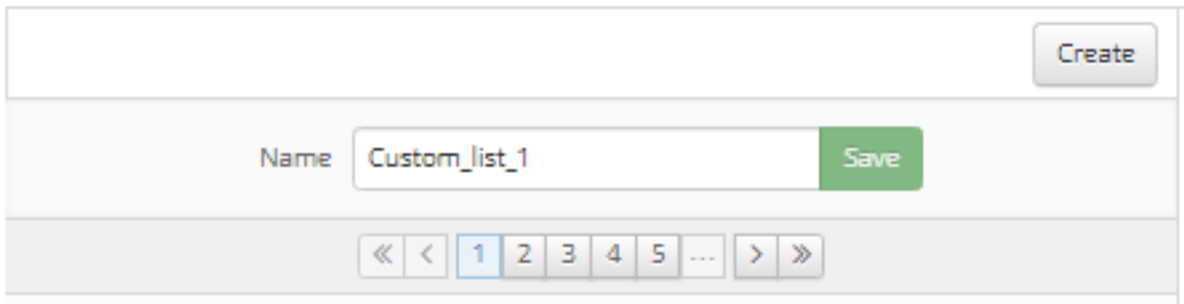
Um eine Liste einfacher benutzerdefinierter Erkennungsoptionen zu erstellen, gehen Sie wie folgt vor:

Schritt 1: Navigieren Sie im AMP-Portal zu **Outbreak Control > Simple (Outbreak-Kontrolle > Einfache Option)**, wie im Bild gezeigt.

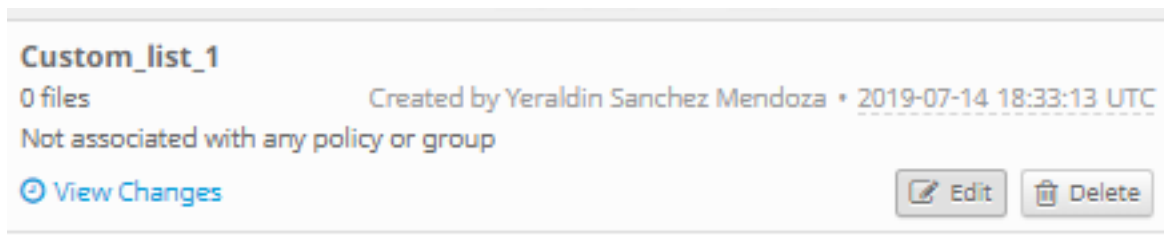


Schritt 2: Klicken Sie auf der Option Benutzerdefinierte Erkennungen - Einfach auf die Schaltfläche **Erstellen**, um eine neue Liste hinzuzufügen, wählen Sie einen Namen aus, um die Liste Einfache benutzerdefinierte Erkennung zu identifizieren und zu speichern, wie im Bild gezeigt.

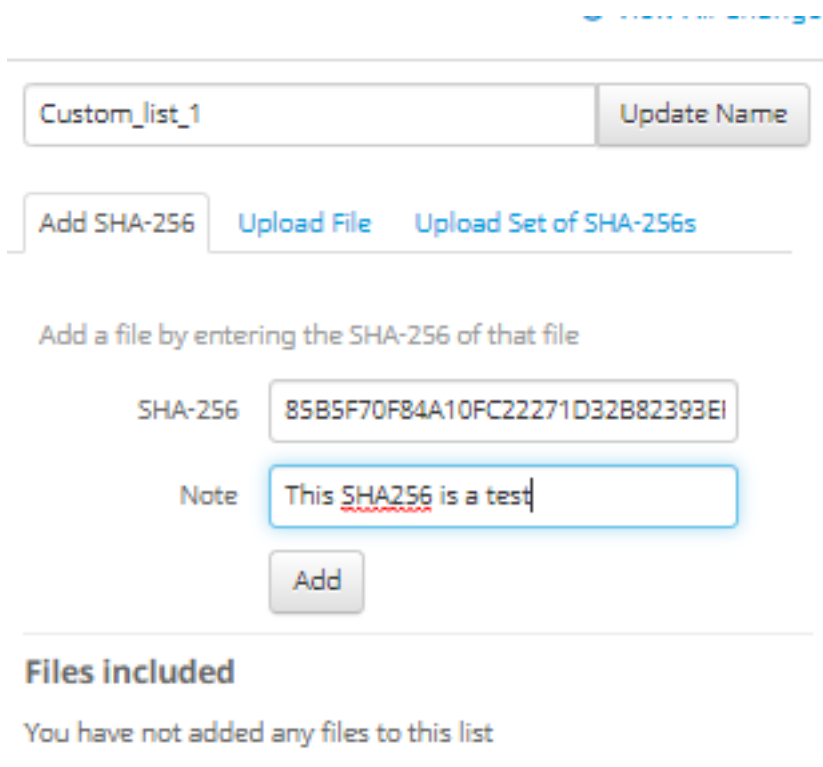
Custom Detections - Simple



Schritt 3: Wenn die Liste erstellt wurde, klicken Sie auf die Schaltfläche **Bearbeiten**, um die Liste der Dateien hinzuzufügen, die Sie blockieren möchten, wie im Bild gezeigt.



Schritt 4: Fügen Sie auf der Option SHA-256 hinzufügen den zuvor aus der zu blockierenden Datei gesammelten SHA-256-Code ein, wie im Bild gezeigt.



Schritt 5: Wählen Sie unter Upload File (Datei hochladen) die Datei aus, die Sie blockieren möchten. Nach dem Hochladen der Datei wird der SHA-256 dieser Datei der Liste hinzugefügt, wie im Bild gezeigt.

[Add SHA-256](#)

[Upload File](#)

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

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

File

No file selected

Browse

Note



Upload

Files included

Schritt 6: Mit der Option SHA-256s hochladen können Sie eine Datei mit einer Liste von zuvor erfassten SHA-256-Codes hinzufügen, wie in den Bildern gezeigt.

SHA256_list.txt - Notepad

File Edit Format View Help

```
85B5F70F84A10FC22271D32B82393EF28CAA55A534F8C08EE3A7DC76139A4DE2  
CEAFF4CD2FDE8B313C52479984E95C0E66A7727313B27516D8F3C70E9F74D71D  
89D599BB4BB64AF353329C1A7D32F1E3FF8C5E0B22D27A4AFEE6A1C3697A0D2A
```

Custom_list_1

Update Name

[Add SHA-256](#)

[Upload File](#)

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

Upload a file containing a set of SHA-256s

File

SHA256_list.txt

Browse

Note

This is the SHA256 list to block

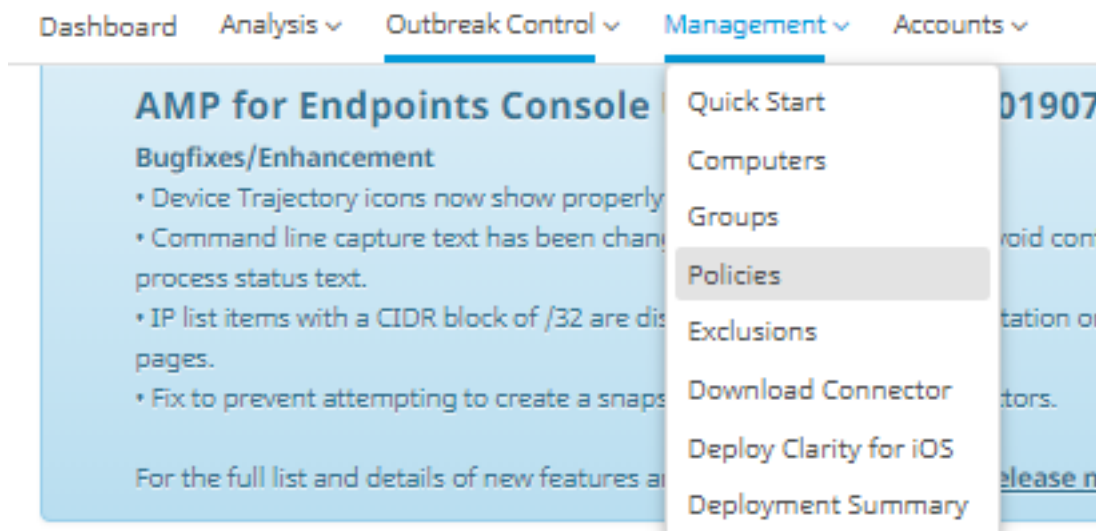


Upload

Files included

Schritt 7: Wenn die Liste Benutzerdefinierte einfache Erkennung erstellt wurde, navigieren Sie zu **Management > Policies (Verwaltung > Richtlinien)**, und wählen Sie die Richtlinie aus, auf die die

zuvor erstellte Liste angewendet werden soll, wie in den Bildern gezeigt.



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

Schritt 8: Klicken Sie auf die Schaltfläche **Bearbeiten**, und navigieren Sie zu **Outbreak Control > Custom Detections - Simple**. Wählen Sie die Liste aus, die zuvor im Dropdown-Menü generiert wurde, und speichern Sie die Änderungen, wie im Bild gezeigt.

< 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

Wenn alle Schritte ausgeführt und die Anschlüsse mit den letzten Richtlinienänderungen synchronisiert wurden, wird die benutzerdefinierte einfache Erkennung wirksam.

Überprüfen

Für diese Konfiguration ist derzeit kein Überprüfungsverfahren verfügbar.

Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.

Warnung: Wenn eine Datei einer Liste einfacher benutzerdefinierter Erkennungsmethoden hinzugefügt wird, muss die Cache-Zeit ablaufen, bevor die Erkennung wirksam wird.

Hinweis: Wenn Sie eine einfache benutzerdefinierte Erkennung hinzufügen, kann sie zwischengespeichert werden. Die Dauer der Zwischenspeicherung einer Datei hängt von ihrer Disposition ab, wie in dieser Liste gezeigt:

·Dateien löschen: 7 Tage

- Unbekannte Dateien: 1 Stunde
- Schädliche Dateien: 1 Stunde