

Configurer une liste de détection personnalisée simple sur le portail AMP for Endpoints

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Flux de travail](#)

[Configuration](#)

[Vérification](#)

[Dépannage](#)

Introduction

Ce document décrit les étapes de création d'une liste de détection personnalisée simple pour détecter, bloquer et mettre en quarantaine des fichiers spécifiques afin d'empêcher les fichiers d'être autorisés sur les périphériques qui ont installé les connecteurs AMP (Advanced Malware Protection) pour les terminaux.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Accès au portail AMP
- Compte avec privilèges d'administrateur
- Taille de fichier maximale de 20 Mo

Components Used

Les informations de ce document sont basées sur la console Cisco AMP for Endpoints version 5.4.20190709.

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 votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Flux de travail

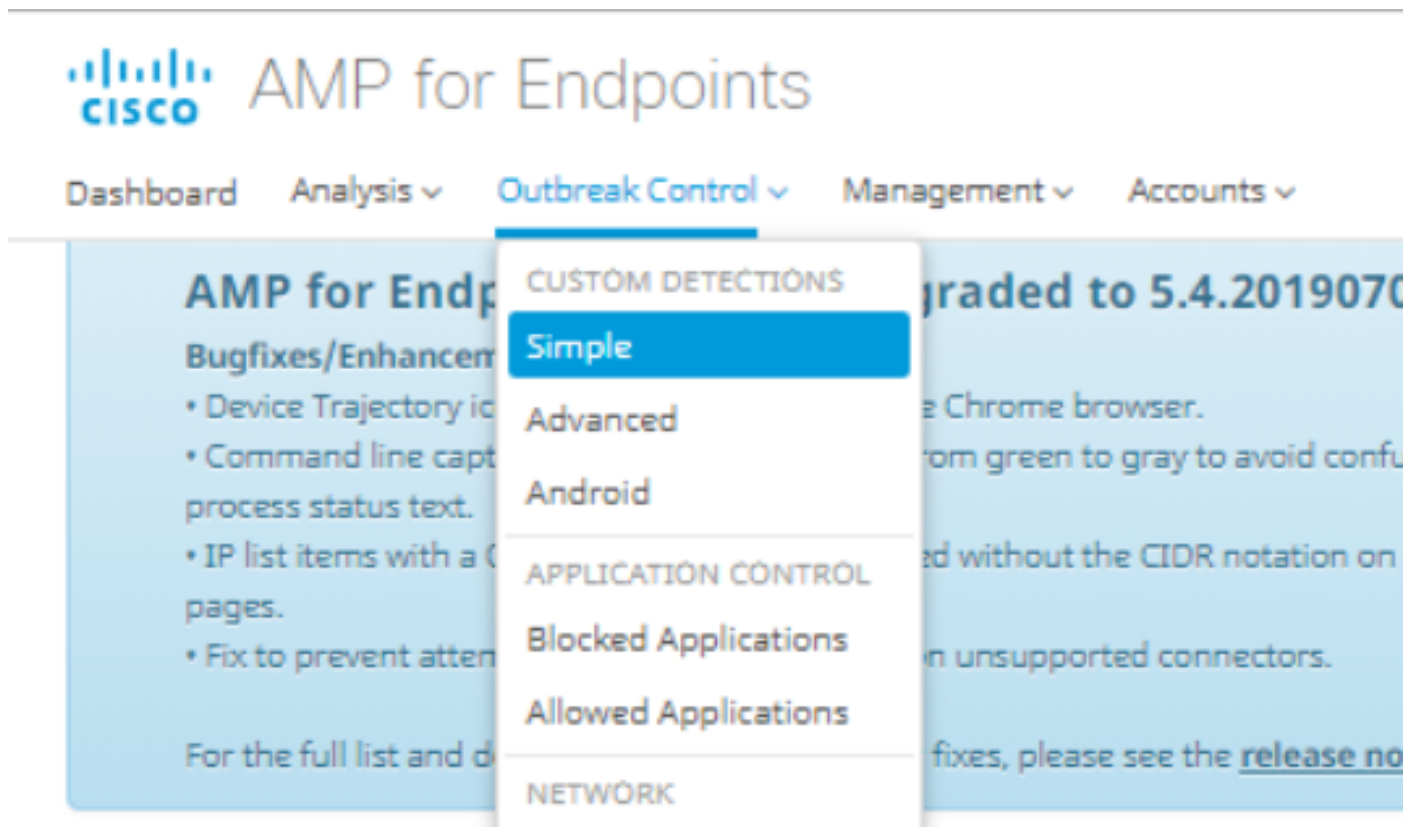
L'option de liste Détection personnalisée simple utilise ce workflow :

- Liste de détection personnalisée simple créée à partir du portail AMP.
- Liste de détection personnalisée simple appliquée dans une stratégie précédemment créée.
- Connecteur AMP installé sur le périphérique et appliqué dans la stratégie.

Configuration

Afin de créer une liste de détection personnalisée simple, procédez comme suit :

Étape 1. Sur le portail AMP, accédez à l'option **Contrôle des attaques > Simple**, comme illustré dans l'image.



Étape 2. Dans l'option Détections personnalisées - Simple, cliquez sur le bouton **Créer** pour ajouter une nouvelle liste, choisissez un nom pour identifier la liste Détection personnalisée simple et enregistrez-la, comme indiqué dans l'image.

Custom Detections - Simple

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

Étape 3. Une fois la liste créée, cliquez sur le bouton **Modifier** pour ajouter la liste des fichiers à bloquer, comme l'illustre l'image.

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](#)

Étape 4. Dans l'option Add SHA-256, collez le code SHA-256 précédemment collecté à partir du fichier spécifique à bloquer, comme illustré dans l'image.

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

Étape 5. Dans l'option Upload File (Télécharger le fichier), recherchez le fichier spécifique à bloquer, une fois le fichier téléchargé, le SHA-256 de ce fichier est ajouté à la liste, comme l'illustre l'image.

[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

Étape 6. L'option Upload Set of SHA-256s permet d'ajouter un fichier avec une liste de plusieurs codes SHA-256 précédemment acquis, comme le montrent les images.

SHA256_list.txt - Notepad

File Edit Format View Help

```
85B5F70F84A10FC22271D32B82393EF28CAA55A534F8C08EE3A7DC76139A4DE2  
CEAFF4CD2FDE8B313C52479984E95C0E66A7727313B27516D8F3C70E9F74D71D  
89D599BB4BB64AF353329C1A7D32F1E3FF8C5E0B22D27A4AFEE6A1C3697A0D2A
```

The screenshot shows a web interface for uploading a custom 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. A 'Note' input field contains 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'.

Étape 7. Une fois la liste Détection personnalisée simple générée, accédez à **Management > Politiques** et choisissez la stratégie dans laquelle vous voulez appliquer la liste précédemment créée, comme le montrent les images.

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 (highlighted), Exclusions, Download Connector, Deploy Clarity for iOS, and Deployment Summary. On the left side of the menu, there is a section titled 'AMP for Endpoints Console Bugfixes/Enhancement' with several bullet points: 'Device Trajectory icons now show properly', 'Command line capture text has been changed', 'process status text.', 'IP list items with a CIDR block of /32 are displayed on the', 'pages.', and 'Fix to prevent attempting to create a snapshot'. At the bottom of this section, it says 'For the full list and details of new features and bugfixes, please see the release notes.'

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

Étape 8. Cliquez sur le bouton **Modifier** et naviguez jusqu'à **Contrôle des attaques > Détections personnalisées - Simple**, sélectionnez la liste précédemment générée dans le menu déroulant et enregistrez les modifications, comme indiqué dans l'image.

< 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

Une fois toutes les étapes effectuées et les connecteurs synchronisés aux dernières modifications de stratégie, la détection personnalisée simple prend effet.

Vérification

Aucune procédure de vérification n'est disponible pour cette configuration.

Dépannage

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.

Avertissement : Si un fichier est ajouté à une liste de détection personnalisée simple, le temps de cache doit expirer avant que la détection ne prenne effet.

Note: Lorsque vous ajoutez une détection personnalisée simple, elle peut être mise en cache. La durée de mise en cache d'un fichier dépend de sa disposition, comme indiqué dans cette liste :

- Nettoyer les fichiers : 7 jours
- Fichiers inconnus : 1 heure
- fichiers malveillants : 1 heure