

# Configure uma lista de detecção personalizada simples no portal AMP para endpoints

## Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Fluxo de trabalho](#)

[Configuração](#)

[Verificar](#)

[Troubleshoot](#)

## Introduction

Este documento descreve as etapas para criar uma lista de Detecção Personalizada Simples para detectar, bloquear e colocar arquivos específicos em quarentena para impedir que os arquivos sejam permitidos em dispositivos que instalaram os conectores da Proteção Avançada contra Malware (AMP) para Endpoints.

## Prerequisites

### Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Acesso ao portal AMP
- Conta com privilégios de administrador
- Tamanho do arquivo não superior a 20 MB

### Componentes Utilizados

As informações neste documento são baseadas no console Cisco AMP para endpoints versão 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. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

## Fluxo de trabalho

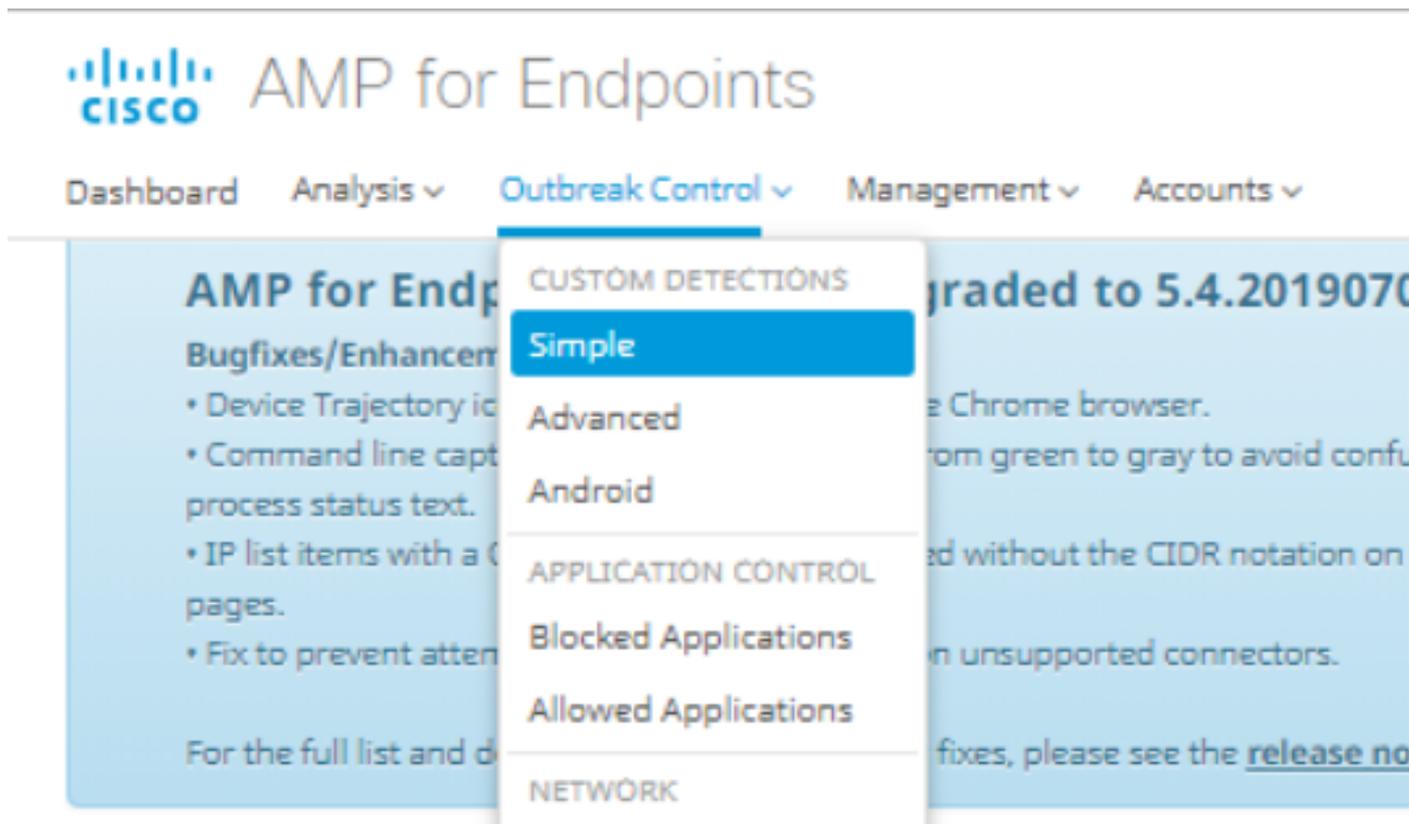
A opção da lista Detecção personalizada simples usa este fluxo de trabalho:

- A lista Simple Custom Detection criada a partir do portal AMP.
- Uma lista de Detecção Personalizada Simples aplicada em uma Política criada anteriormente.
- O conector AMP instalado no dispositivo e aplicado na política.

## Configuração

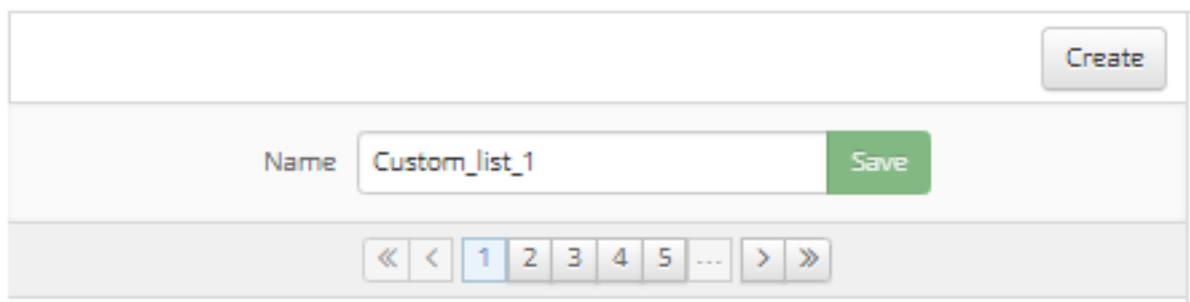
Para criar uma lista de Detecção personalizada simples, siga estas etapas:

Etapa 1. No portal AMP, navegue até a opção **Controle de ataque > Simples**, como mostrado na imagem.



Etapa 2. Na opção Custom Detections - Simple (Detecções personalizadas - Simples), clique no botão **Create** para adicionar uma nova lista, escolha um nome para identificar a lista Simple Custom Detection (Detecção personalizada simples) e salve-a, como mostrado na imagem.

### Custom Detections - Simple

A screenshot of the 'Custom Detections - Simple' configuration page. At the top right is a 'Create' button. Below it is a 'Name' field containing the text 'Custom\_list\_1' and a green 'Save' button. At the bottom, there is a pagination control showing page 1 of 5.

Etapa 3. Quando a lista for criada, clique no botão **Editar** para adicionar a lista dos arquivos que deseja bloquear, como mostrado na imagem.

**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](#)

Etapa 4. Na opção Add SHA-256, cole o código SHA-256 anteriormente coletado do arquivo específico que você deseja bloquear, como mostrado na imagem.

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

Etapa 5. Na opção Carregar arquivo, procure o arquivo específico que deseja bloquear, assim que o arquivo for carregado, o SHA-256 desse arquivo será adicionado à lista, como mostrado na imagem.

[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**

Etapa 6. A opção Carregar conjunto de SHA-256s permite adicionar um arquivo com uma lista de vários códigos SHA-256 adquiridos anteriormente, como mostrado nas imagens.

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' text area 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'.

Passo 7. Quando a lista Detecção personalizada simples for gerada, navegue para **Gerenciamento > Políticas** e escolha a política na qual deseja aplicar a lista criada anteriormente, como mostrado nas imagens.

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 interface, there is a section titled 'AMP for Endpoints Console' with a sub-section 'Bugfixes/Enhancement' containing several bullet points. On the right side, there is a partially visible section with the number '01907' and some text.

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

Etapa 8. Clique no botão **Editar** e navegue para **Controle de epidemia > Detecções personalizadas - Simples**, selecione a lista gerada anteriormente no menu suspenso e salve as alterações, como mostrado na imagem.

## < 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
<b>Outbreak Control</b>	Application Control - Allowed None
Product Updates	Application Control - Blocked leisanch_blocking2
Advanced Settings	Network - IP Block & Allow Lists None

Clear Select Lists

Cancel Save

Quando todas as etapas são executadas e os conectores são sincronizados com as últimas alterações de política, a Detecção personalizada simples entra em vigor.

## Verificar

No momento, não há procedimento de verificação disponível para esta configuração.

## Troubleshoot

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.

**aviso:** Se um arquivo for adicionado a uma lista de Detecção personalizada simples, o tempo de cache deverá expirar antes que a detecção entre em vigor.

**Note:** Quando você adiciona uma Detecção personalizada simples, ela está sujeita a ser armazenada em cache. O tempo durante o qual um arquivo é armazenado em cache depende de sua disposição, como mostrado nesta lista:

Limpar arquivos: 7 dias

Arquivos desconhecidos: 1 hora

Arquivos mal-intencionados: 1 hora