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

Contents

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

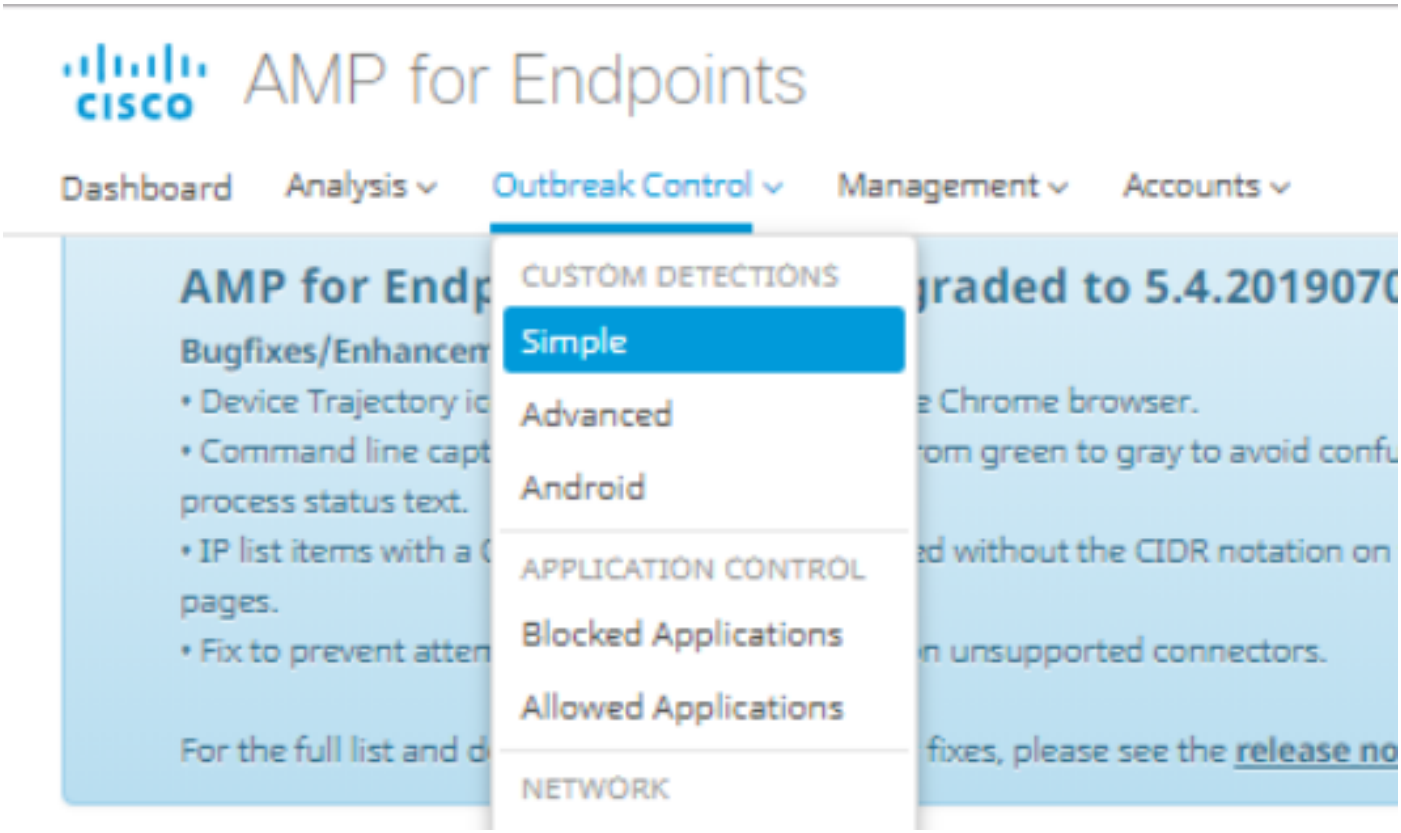
A opção da lista Detecção personalizada simples usa este fluxo de trabalho:

- 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.

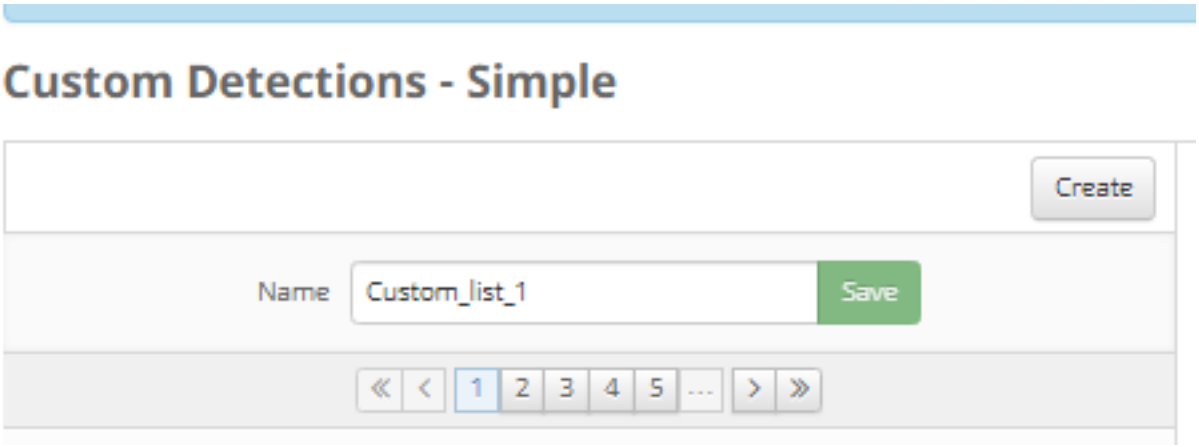
Configuração

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

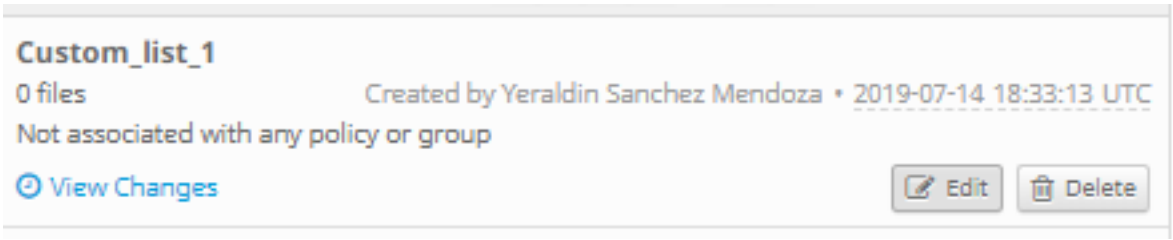
Etapa 1. No portal AMP, navegue até a opção **Controle de ataque > Simples**, como mostrado na imagem.



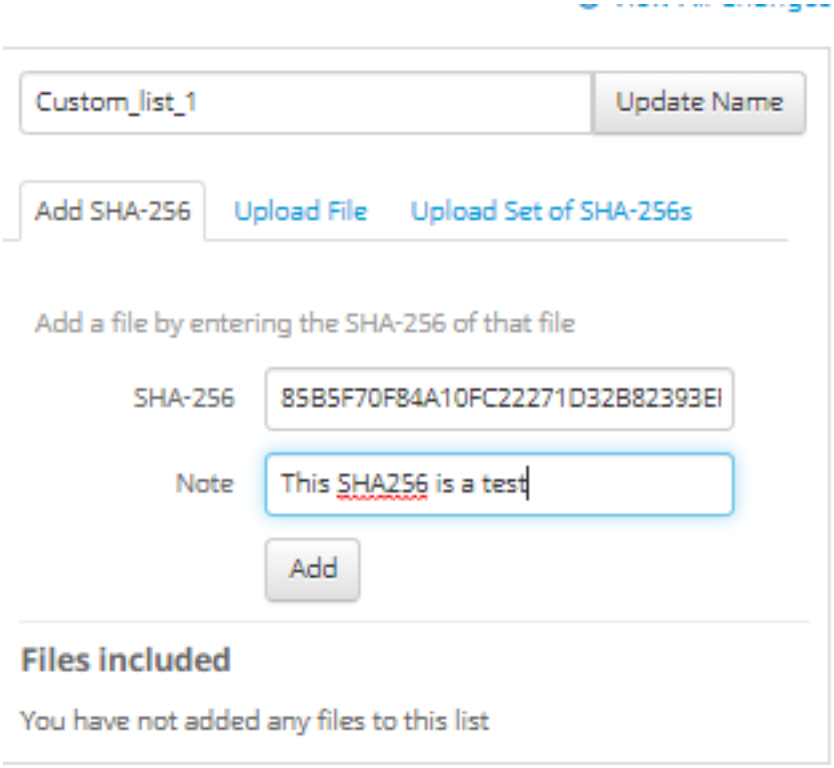
Etapa 2. Na opção Custom Detections - Simple (Detecções personalizadas - Simples), clique no botão **Create** para adicionar uma nova lista, escolha um nome para identificar a lista Simple Custom Detection (Detecção personalizada simples) e salve-a, como mostrado na imagem.



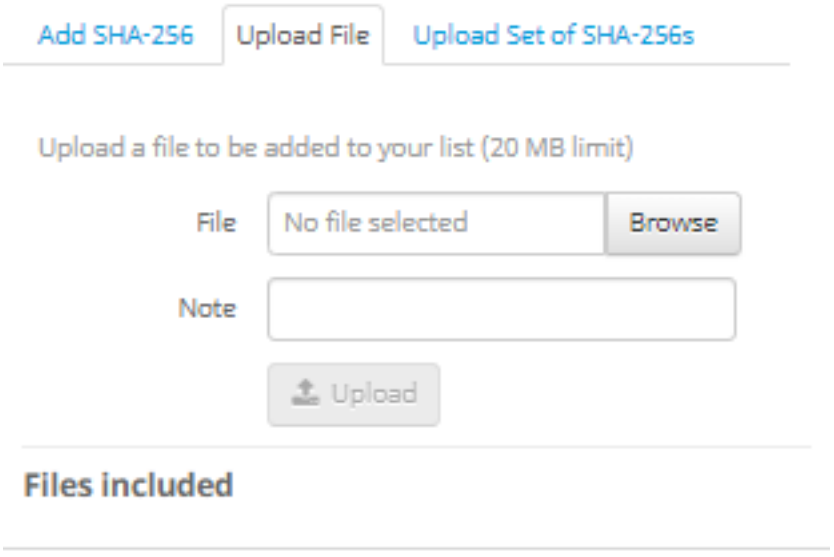
Etapa 3. Quando a lista for criada, clique no botão **Editar** para adicionar a lista dos arquivos que deseja bloquear, como mostrado na imagem.



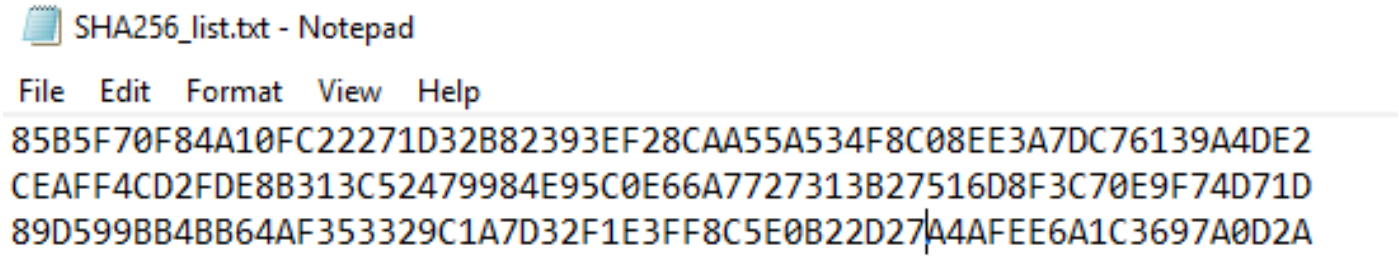
Etapa 4. Na opção Add SHA-256, cole o código SHA-256 anteriormente coletado do arquivo específico que você deseja bloquear, como mostrado na imagem.

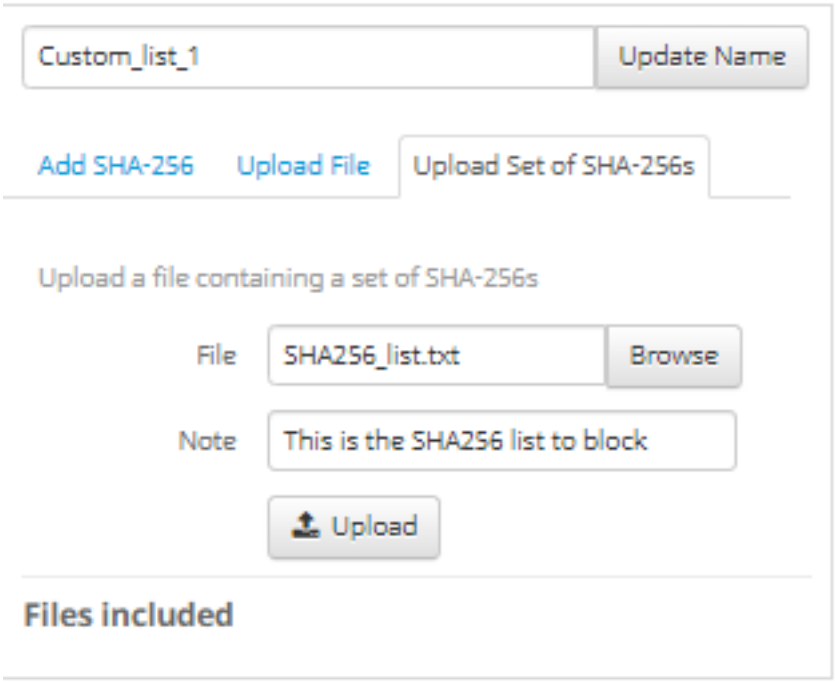


Etapa 5. Na opção Carregar arquivo, procure o arquivo específico que deseja bloquear, assim que o arquivo for carregado, o SHA-256 desse arquivo será adicionado à lista, como mostrado na imagem.

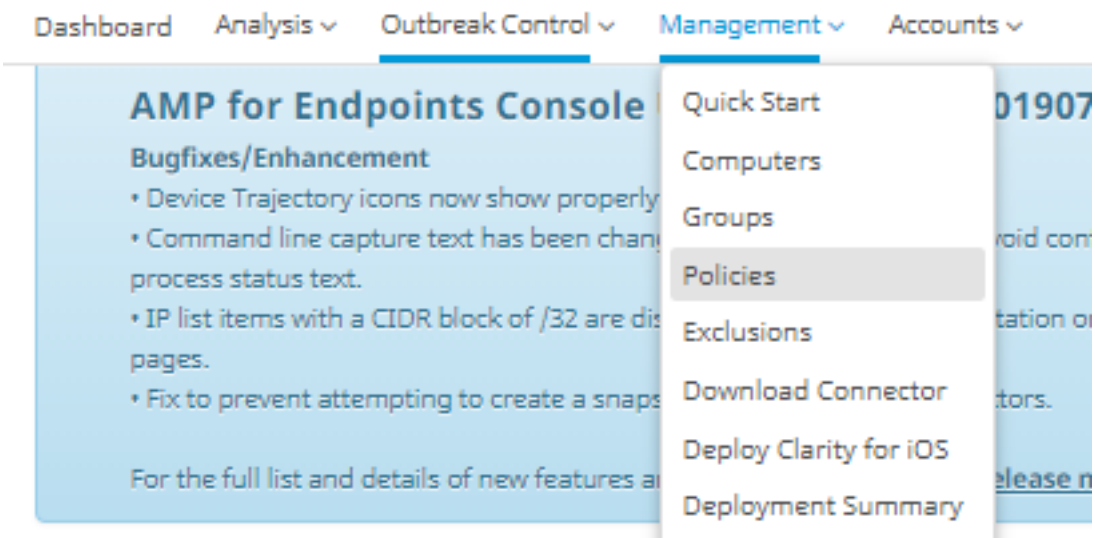


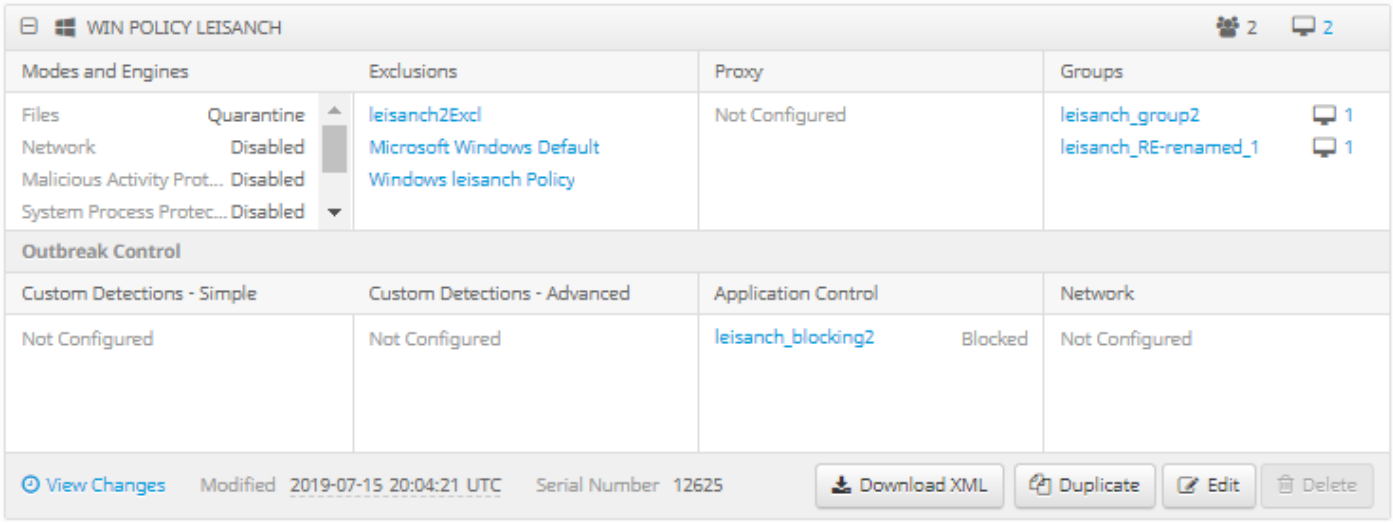
Etapa 6. A opção Carregar conjunto de SHA-256s permite adicionar um arquivo com uma lista de vários códigos SHA-256 adquiridos anteriormente, como mostrado nas imagens.



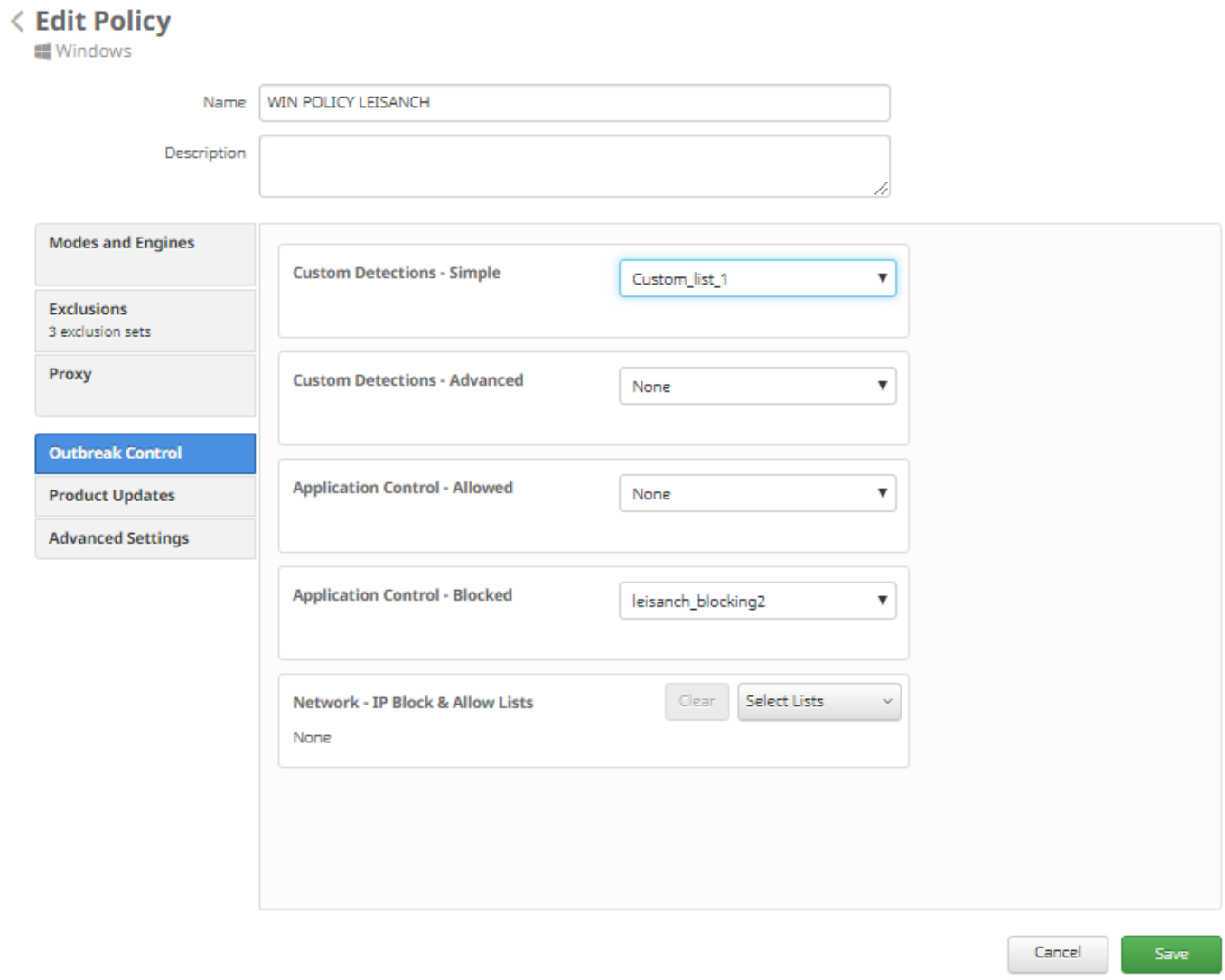


Passo 7. Quando a lista Detecção personalizada simples for gerada, navegue para **Gerenciamento > Políticas** e escolha a política na qual deseja aplicar a lista criada anteriormente, como mostrado nas imagens.





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.



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