

在面向终端的AMP门户上配置简单自定义检测列表

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[工作流](#)

[配置](#)

[验证](#)

[故障排除](#)

简介

本文档介绍创建简单自定义检测列表的步骤，以检测、阻止和隔离特定文件，防止在已安装面向终端的高级恶意软件防护(AMP)连接器的设备上允许文件。

先决条件

要求

Cisco 建议您了解以下主题：

- 访问AMP门户
- 具有管理员权限的帐户
- 文件大小不超过20 MB

使用的组件

本文档中的信息基于面向终端的思科AMP控制台版本5.4.20190709。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

工作流

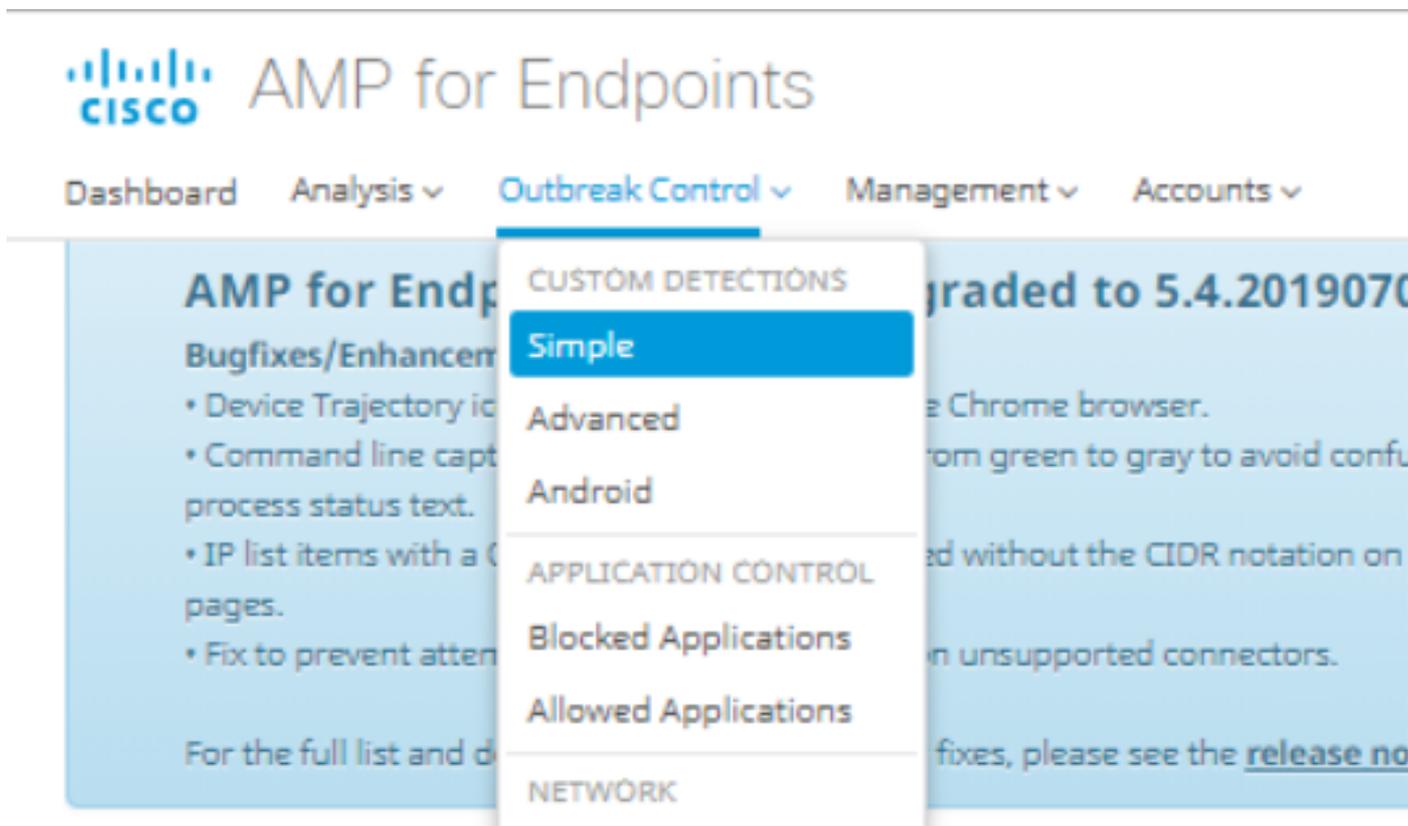
“简单自定义检测”(Simple Custom Detection)列表选项使用此工作流程：

- 从AMP门户创建的简单自定义检测列表。
- 在之前创建的策略中应用的简单自定义检测列表。
- AMP连接器安装在设备上并应用在策略中。

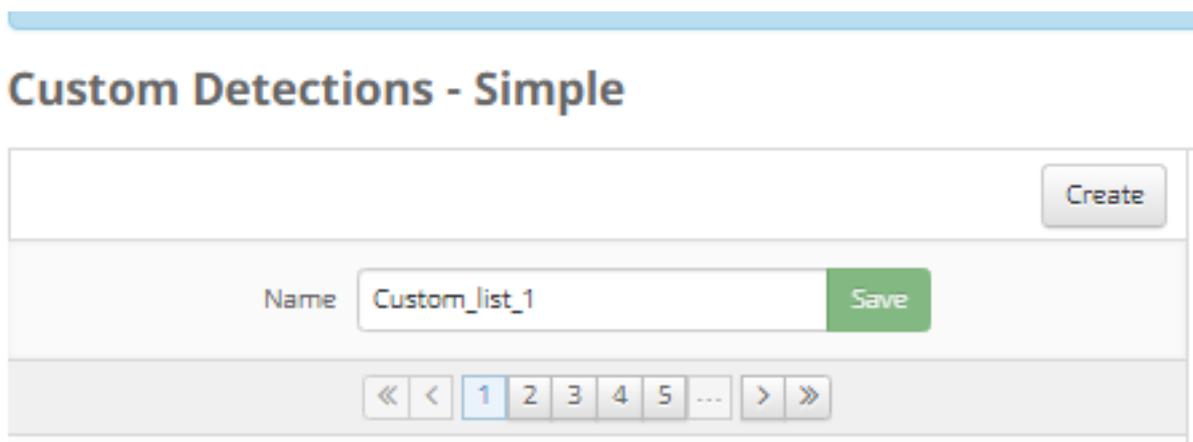
配置

要创建简单自定义检测列表，请执行以下步骤：

步骤1.在AMP门户上，导航至**Outbreak Control > Simple**选项，如图所示。



步骤2.在“自定义检测 — 简单”选项上，单击**创建**按钮以添加新列表，选择一个名称以标识“简单自定义检测”列表并保存，如图所示。



步骤3.创建列表后，单击“编辑”按钮，添加要阻止的文件列表，如图所示。



步骤4.在Add SHA-256选项上，粘贴之前从要阻止的特定文件收集的SHA-256代码，如图所示。

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 85B5F70F84A10FC22271D32B82393EI

Note This SHA256 is a test

Add

Files included

You have not added any files to this list

步骤5.在Upload File选项上，浏览要阻止的特定文件，文件上传后，此文件的SHA-256将添加到列表中，如图所示。

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

步骤6. Upload Set of SHA-256s (上传SHA-256s集)选项允许添加一个文件，其中包含之前获取的多个SHA-256代码的列表，如图所示。

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

步骤7.生成“简单自定义检测”列表后，导航到**管理>策略**并选择要应用之前创建的列表的策略，如图所示。

Dashboard Analysis ▾ Outbreak Control ▾ Management ▾ Accounts ▾

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 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

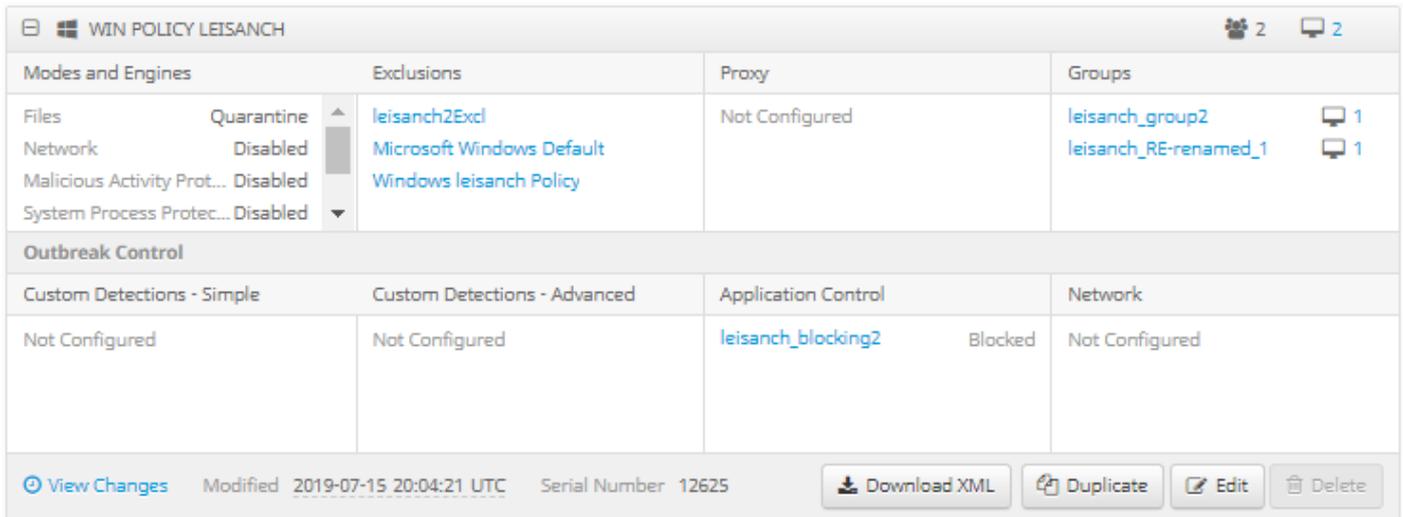
Policies

Exclusions

Download Connector

Deploy Clarity for iOS

Deployment Summary



步骤8.单击Edit按钮并导航到Outbreak Control > Custom Detections - Simple，选择之前在下拉菜单上生成的列表并保存更改，如图所示。

< 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

执行所有步骤并将连接器同步到上次策略更改后，简单自定义检测生效。

验证

当前没有可用于此配置的验证过程。

故障排除

目前没有针对此配置的故障排除信息。

警告： 如果将文件添加到简单自定义检测列表，则缓存时间必须在检测生效之前过期。

注意： 添加简单自定义检测时，它将被缓存。文件缓存的时间长度取决于其性质，如以下列表所示：

- 干净文件：7 天
- 未知文件：1 小时
- 恶意文件：1 小时