Configure a Simple Custom Detection List on the AMP for Endpoints Portal

Contents

Introduction

This document describes the steps to create a Simple Custom Detection list to detect, block and quarantine specific files to prevent the files to be allowed on devices that have installed the Advanced Malware Protection (AMP) for Endpoints connectors.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Access to the AMP portal
- Account with administrator privileges
- File size no more than 20 MB

Components Used

The information in this document is based on Cisco AMP for Endpoints console 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. If your network is live, ensure that you understand the potential impact of any command.

Workflow

The Simple Custom Detection list option uses this workflow:

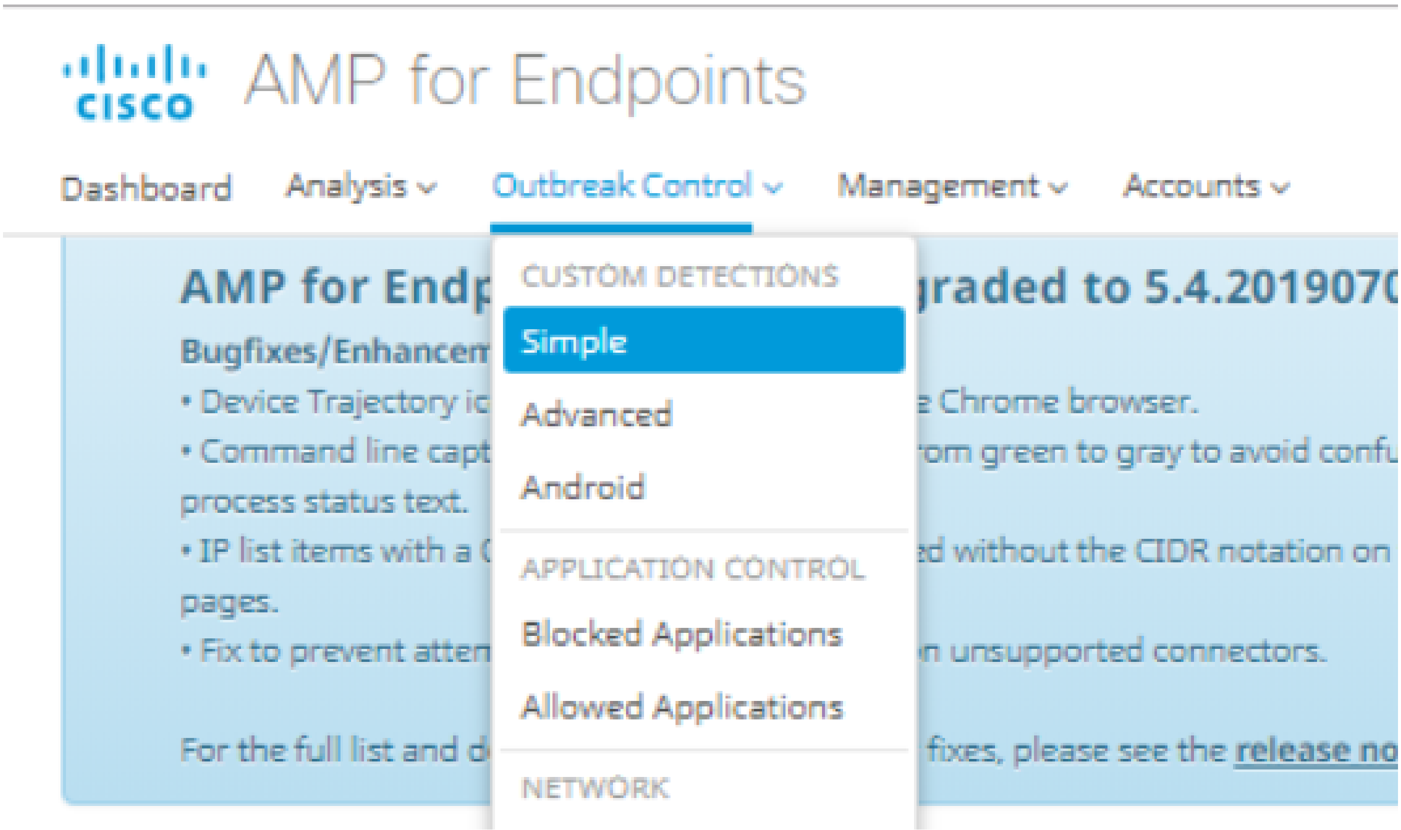
- The Simple Custom Detection list created from the AMP portal.

- A Simple Custom Detection list applied in a Policy previously created.
- The AMP Connector installed on the device and applied in the Policy.

Configuration

In order to create a Simple Custom Detection list, follow these steps:

Step 1. On the AMP Portal, navigate to **Outbreak Control > Simple** option, as shown in the image.



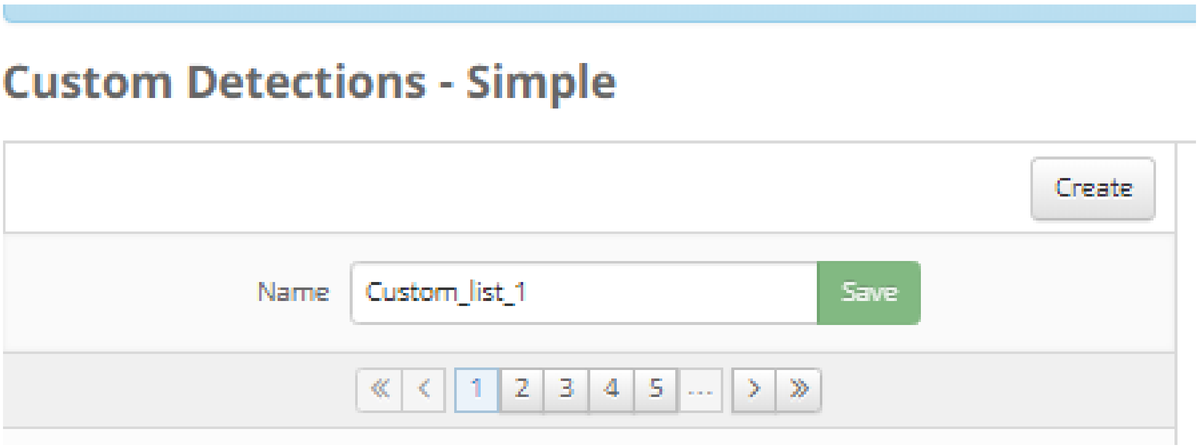
AMP for Endp... ...graded to 5.4.2019070...

Bugfixes/Enhancem...

- Device Trajectory ic... ...e Chrome browser.
- Command line capt... ...om green to gray to avoid confu... process status text.
- IP list items with a ... ...ed without the CIDR notation on ... pages.
- Fix to prevent atten... ...n unsupported connectors.

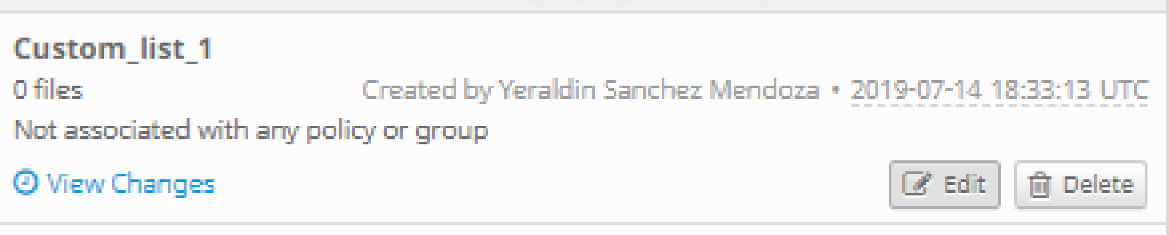
For the full list and d... ...fixes, please see the release no...

Step 2. On the Custom Detections – Simple option, click **Create** button to add a new list, choose a name to identify the Simple Custom Detection list and save it, as shown in the image.



Name: Custom_list_1

Step 3. Once the list is created, click on the **Edit** button to add the list of the files you want to block, as shown in the image.

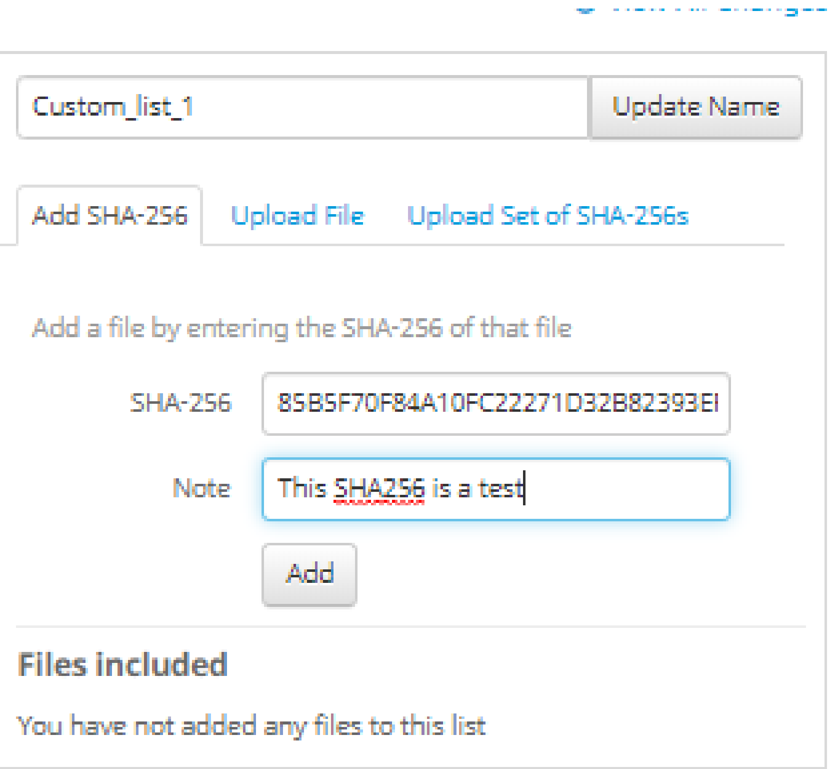


Custom_list_1

0 files   Created by Yeraldin Sanchez Mendoza • 2019-07-14 18:33:13 UTC

Not associated with any policy or group

Step 4. On the Add SHA-256 option, paste the SHA-256 code previously collected from the specific file you want to block, as shown in the image.



Custom_list_1

Add a file by entering the SHA-256 of that file

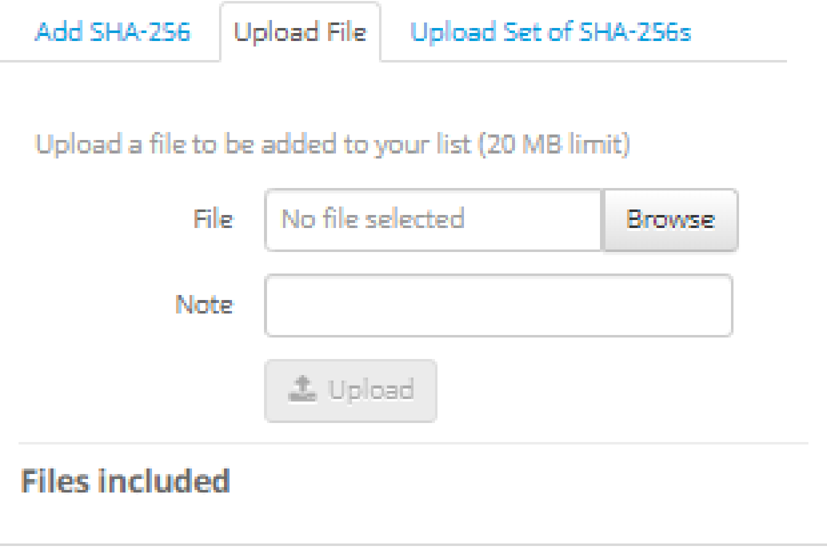
SHA-256: 85B5F70F84A10FC22271D32B82393EI

Note: This SHA256 is a test

Files included

You have not added any files to this list

Step 5. On the Upload File option, browse for the specific file that you want to block, once the file is uploaded, the SHA-256 of this file is added into the list, as shown in the image.



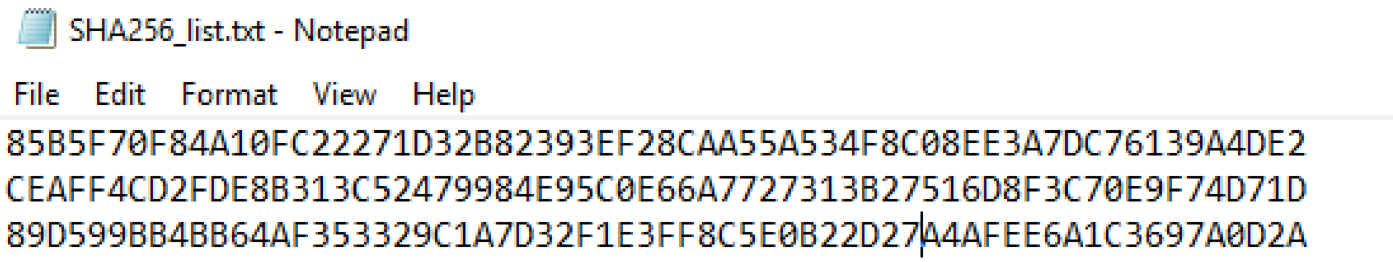
Upload a file to be added to your list (20 MB limit)

File: No file selected

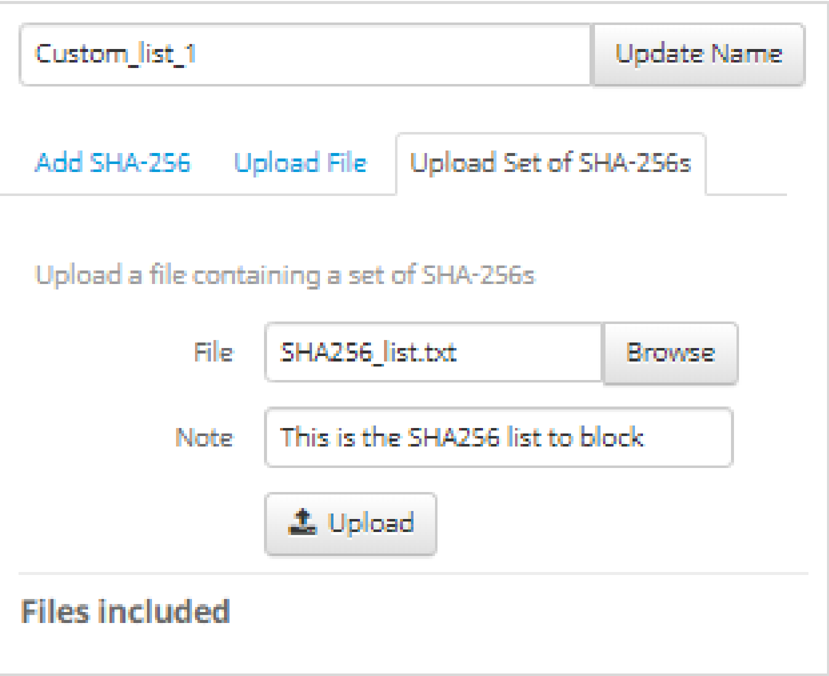
Note:

Files included

Step 6. The Upload Set of SHA-256s option allows to add a file with a list of multiple SHA-256 codes previously acquired, as shown in the images.



```
85B5F70F84A10FC22271D32B82393EF28CAA55A534F8C08EE3A7DC76139A4DE2
CEAFF4CD2FDE8B313C52479984E95C0E66A7727313B27516D8F3C70E9F74D71D
89D599BB4BB64AF353329C1A7D32F1E3FF8C5E0B22D27A4AFEE6A1C3697A0D2A
```



Custom_list_1

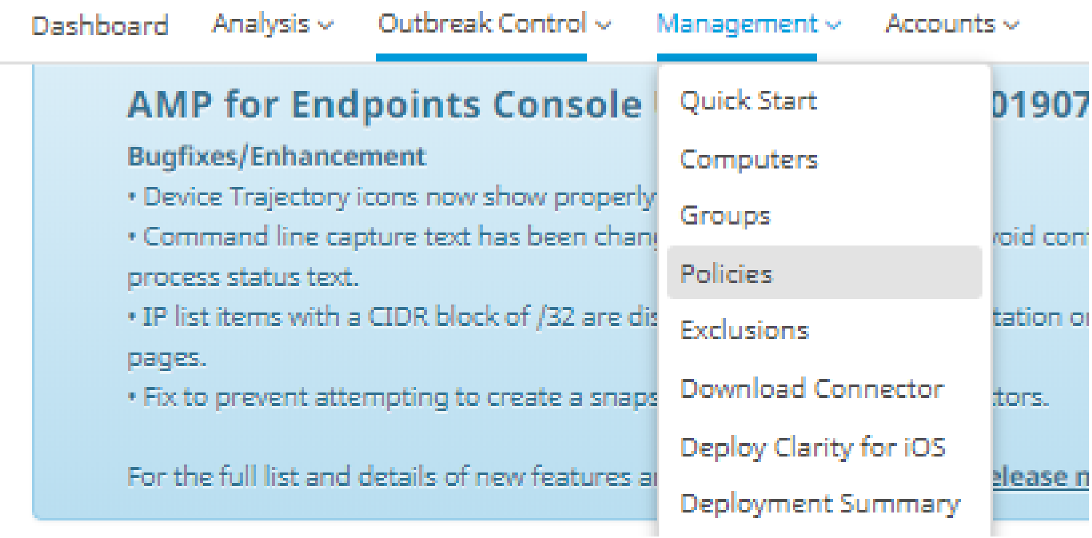
Upload a file containing a set of SHA-256s

File: SHA256_list.txt

Note: This is the SHA256 list to block

Files included

Step 7. Once the Simple Custom Detection list is generated, navigate to **Management > Policies** and choose the policy where you want to apply the list previously created, as shown in the images.

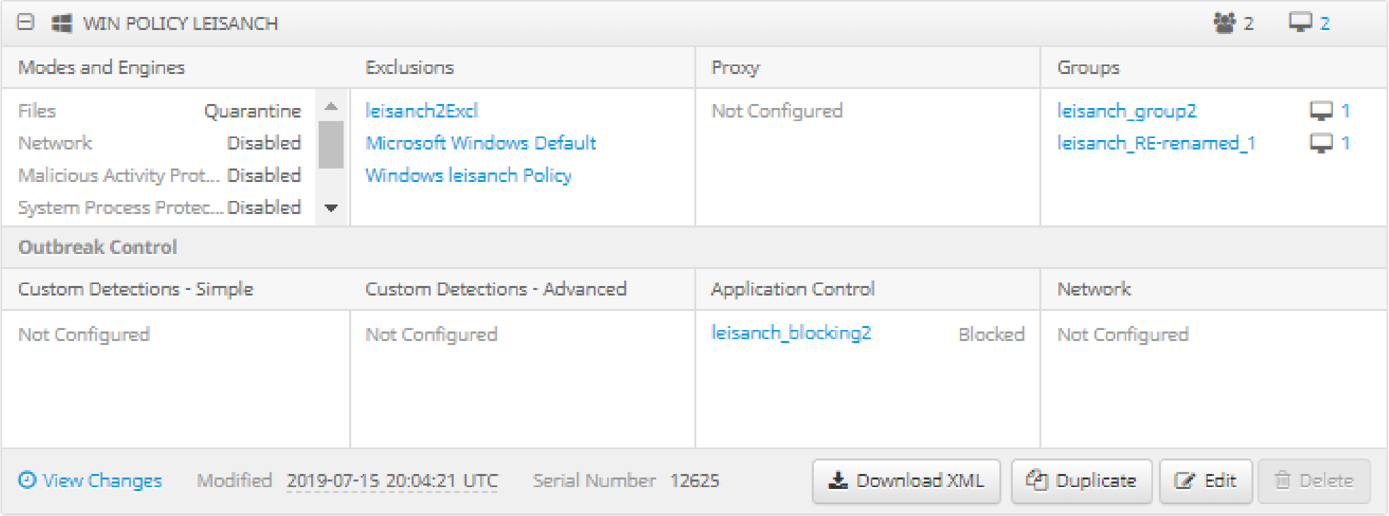


AMP for Endpoints Console … 01907

Bugfixes/Enhancement

- Device Trajectory icons now show properly …
- Command line capture text has been chan… …oid com… process status text.
- IP list items with a CIDR block of /32 are dis… …tation o… pages.
- Fix to prevent attempting to create a snaps… …tors.

For the full list and details of new features a… …elease n…



WIN POLICY LEISANCH — 2 — 2

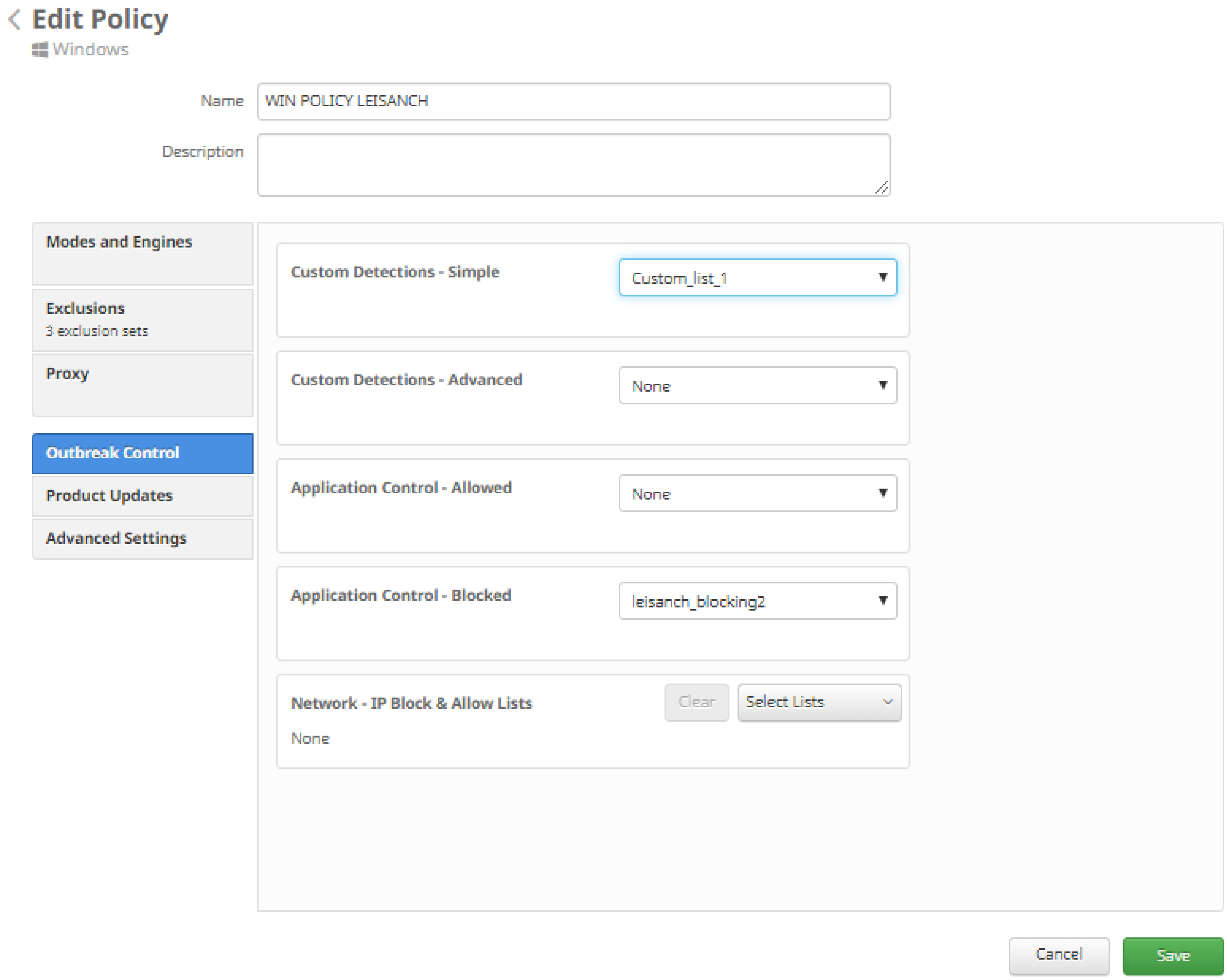
Modes and Engines	Exclusions	Proxy	Groups
Files: Quarantine Network: Disabled Malicious Activity Prot...: Disabled System Process Protec...: Disabled	leisanch2Excl Microsoft Windows Default Windows leisanch Policy	Not Configured	leisanch_group2 — 1 leisanch_RE-renamed_1 — 1

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

Step 8. Click on the **Edit** button and navigate to **Outbreak Control > Custom Detections – Simple,** select the list previously generated on the drop-down menu and save the changes, as shown in the image.



Edit Policy
Windows

Name: WIN POLICY LEISANCH

Description:

Custom Detections - Simple: Custom_list_1

Custom Detections - Advanced: None

Application Control - Allowed: None

Application Control - Blocked: leisanch_blocking2

Network - IP Block & Allow Lists: None

Once all steps are performed, and the connectors are synchronized to the last policy changes, the Simple Custom Detection takes effect.

Verify

There is currently no verification procedure available for this configuration.

Troubleshoot

There is currently no specific troubleshooting information available for this configuration.

> **Warning**: If a file is added to a Simple Custom Detection list, the cache time must expire before the detection takes effect.

> **Note**: When you add a Simple Custom Detection, it is subject to be cached. The length of time a file is cached depends on its disposition, as shown in this list:
> - Clean files: 7 days
> - Unknown files: 1 hour
> - Malicious files: 1 hour