

# Configure and Manage Exclusions in Cisco Secure Endpoint Connector

## Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Secure Endpoint workflow](#)

[Cisco Maintained Exclusions](#)

[Custom Exclusions](#)

[Secure Endpoint engine](#)

[Path Exclusion](#)

[Wildcard Exclusion](#)

[File Extension Exclusion](#)

[Process: File Scan Exclusion](#)

[System Process Protection \(SPP\)](#)

[SPP Exclusion](#)

[Malicious Activity Protection \(MAP\)](#)

[MAP Exclusion](#)

[Exploit Prevention \(Exprev\)](#)

[Behavioral Protection \(BP\)](#)

[Related Information](#)

## Introduction

This document describes how to create the exclusion for the different engines on the Cisco Secure Endpoint console.

## Prerequisites

### Requirements

Cisco recommends that you have knowledge of these topics:

- Modify and apply an exclusion list to a policy in the Secure Endpoint console
- Windows CSIDL convention

### Components Used

The information in this document is based on these software and hardware versions:

- Cisco Secure Endpoint console 5.4.20211013
- Secure Endpoint User Guide revision Oct 15, 2021

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.

# Secure Endpoint workflow

In a high level of operations the Cisco Secure Endpoint processes a file Secure Hash Algorithm (SHA) in this order through the main components of the connector:

- Exclusions
- Tetra Engine
- Application control (Allow list / Blocklist)
- SHA Engine
- Exploit prevention (Exprev) / Malicious Activity Protection (MAP) / System Process Protection / Network engine (Device Flow Correlation)

---

**Note:** Exclusion or Allow/Blocklist creation depends on which engine detected the file.

---

## Cisco Maintained Exclusions

Cisco-Maintained Exclusions are created and maintained by Cisco to provide better compatibility between the Secure Endpoint Connector and antivirus, and security products, or other software.

These exclusion sets contain different types of exclusions to ensure proper operation.

You can track the changes performed to these exclusions in the article [Cisco-Maintained Exclusion List Changes for Cisco Secure Endpoint Console](#).

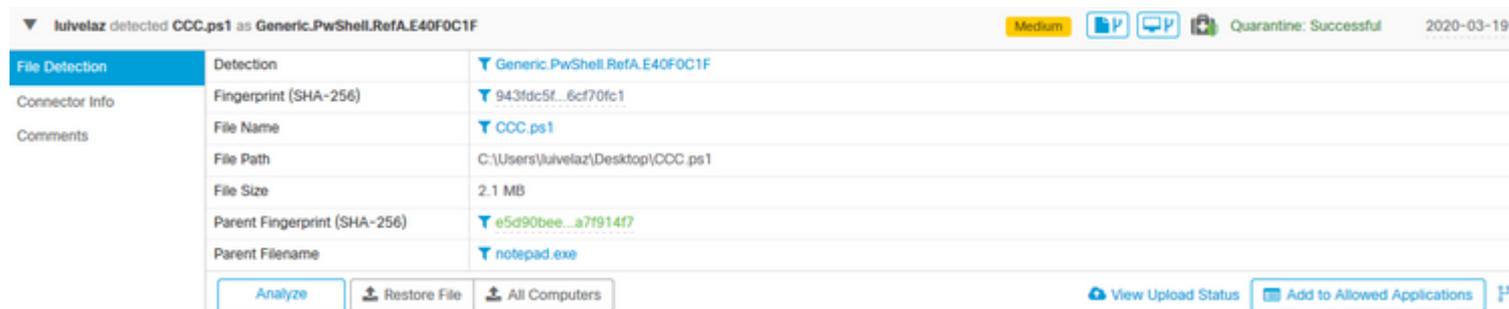
## Custom Exclusions

### Secure Endpoint engine

File Scan (CPU usage / File detections) by Tetra & SHA engine:

Use these types of exclusions to avoid detection/quarantine of a file or to [mitigate Secure Endpoint high CPU](#).

The event on the Secure Endpoint console is as shown in the image.



The screenshot displays a file detection event in the Cisco Secure Endpoint console. The event details are as follows:

File Detection	Detection	Generic.PwShell.RefA.E40F0C1F
Connector Info	Fingerprint (SHA-256)	943fdc5f...6cf70fc1
Comments	File Name	CCC.ps1
	File Path	C:\Users\luvelaz\Desktop\CCC.ps1
	File Size	2.1 MB
	Parent Fingerprint (SHA-256)	e5d90bee...a7f914f7
	Parent Filename	notepad.exe

At the bottom of the event details, there are buttons for "Analyze", "Restore File", and "All Computers". On the right side, there are buttons for "View Upload Status" and "Add to Allowed Applications".

---

**Note:** CSIDL can be used for exclusions, please refer to [this](#) Microsoft document for more information on CSIDL.

---

### Path Exclusion

Path	C:\Users\luivelaz\Desktop\CCC.ps1
------	-----------------------------------

### Wildcard Exclusion

Wildcard	C:\Users\*\Desktop\CCC.ps1
	<input type="checkbox"/> Apply to all drive letters

**Note:** Option **Apply to all drive letters** is used to also apply the exclusion to drives [A-Z] attached to the system.

### File Extension Exclusion

File Extension	.ps1
----------------	------

**Caution:** Use this type of exclusion with caution as it excludes all files with the file extension from scans regardless of the path location.

### Process: File Scan Exclusion

Process	Path	C:\Path\to\executable.exe
File Scan	SHA	
	You can provide path and/or SHA-256. If you specify both a path and SHA-256 then both conditions must be met for the process to be excluded.	
	<input checked="" type="checkbox"/> Apply to child processes	

### System Process Protection (SPP)

System Process Protection engine is available from connector version 6.0.5 and it protects the next Windows processes:

- Session Manager Subsystem (sms.exe)
- Client/Server Runtime Subsystem (csrss.exe)
- Local Security Authority Subsystem (lsass.exe)
- Windows Logon Application (winlogon.exe)
- Windows Start-up Application (wininit.exe)

This image shows an SPP event.

Event Details	Fingerprint (SHA-256)	aa52b2d3...acee8d21
Connector Info	File Name	lsass.exe
Comments	File Path	C:\Windows\System32\lsass.exe
	File Size	56.73 KB
	Reason	Process module is not clean and not signed
	Parent Fingerprint (SHA-256)	f3c7b460...fd3b16dd
	Parent Filename	TestAMPprotect.exe
	Parent File Size (bytes)	1608704
<input type="button" value="Analyze"/>		

### SPP Exclusion

Process	Path	Path\to\the\executable.exe
System Process	SHA	
	You can provide path and/or SHA-256. If you specify both a path and SHA-256 then both can be met for the process to be excluded.	
	<input checked="" type="checkbox"/> Apply to child processes	

Process	Path	
System Process	SHA	SHA-256 of the file (From the Parent Filename field)
	not a valid SHA-256	
	You can provide path and/or SHA-256. If you specify both a path and SHA-256 then both can be met for the process to be excluded.	
<input checked="" type="checkbox"/> Apply to child processes		

### Malicious Activity Protection (MAP)

Malicious Activity Protection (MAP) engine, defends your endpoint from a ransomware attack. It identifies malicious actions or processes when they execute, and protects your data against encryption.

A MAP event is shown in this image.

Malicious Activity Protection	Fingerprint (SHA-256)	9967155a...2956d820
Connector Info	Affected Files Count	5
Comments	Affected Files	C:\Users\umontero\Desktop\Test files\AMP4E-8120-SPP-MAP-EXPREV-test_files\Map\rewrite_data\1.txt.new C:\Users\umontero\Desktop\Test files\AMP4E-8120-SPP-MAP-EXPREV-test_files\Map\rewrite_data\0.txt.new C:\Users\umontero\Desktop\Test files\AMP4E-8120-SPP-MAP-EXPREV-test_files\Map\rewrite_data\4.txt.new C:\Users\umontero\Desktop\Test files\AMP4E-8120-SPP-MAP-EXPREV-test_files\Map\rewrite_data\2.txt.new C:\Users\umontero\Desktop\Test files\AMP4E-8120-SPP-MAP-EXPREV-test_files\Map\rewrite_data\3.txt.new
	File Name	rewrite.exe
	File Path	C:\Users\umontero\Desktop\Test files\AMP4E-8120-SPP-MAP-EXPREV-test_files\Map\rewrite.exe
	File Size	4.37 MB
	Parent Fingerprint (SHA-256)	9967155a...2956d820
	Parent Filename	rewrite.exe
<div style="display: flex; justify-content: space-between;"> <span>Analyze</span> <span>Restore File</span> <span>All Computers</span> </div>		

## MAP Exclusion

Process	Path	Path\to\the\executable.exe
Malicious Activity	SHA	
<p>You can provide path and/or SHA-256. If you specify both a path and SHA-256 then both conditions must be met for the process to be excluded.</p>		
<input checked="" type="checkbox"/> Apply to child processes		

**Caution:** Use this type of exclusion with caution and after you confirm that the detection is indeed not malicious.

## Exploit Prevention (Exprev)

The exploit prevention engine defends your endpoints from memory injection attacks commonly used by malware and other zero-day attacks on unpatched software vulnerabilities. When it detects an attack against a protected process it will be blocked and generate an event but there will not be a quarantine.

An Exprev event is shown in this image.

Testing.machine1.amp.com prevented an exploit in CUDL.LOS.exe process.

Exploit Prevention	Fingerprint (SHA-256)	ab6b87b8...3e70e087
Connector Details	Attacked Module	c:\program files (x86)\adobe\acrobat dc\acrobat\bib.dll
Comments	Application	CUDL.LOS.exe
	Base Address	0x7C700000
	File Name	CUDL.LOS.exe
	File Path	C:\Users\mabat\AppData\Local\Apps\2.0\E9781GXN.CJV\80XQ3X5B.94H\len
	File Size	5.82 MB
	Parent Fingerprint (SHA-256)	375a7501...e8624659
	Parent Filename	dfsvc.exe
	Parent File Size	24.27 KB

Analyze

## Exprev exclusion

Executable	Name	CUDL.LOS.exe
Exploit Prevention	Provide an executable name to be excluded from protection by the Exploit Prevention (ValidExecutable.exe).	

+ Add Exclusion    + Add Multiple Exclusions...

**Caution:** Use this exclusion whenever you trust the activity on the affected module/application.

## Behavioral Protection (BP)

The behavioral protection engine enhances the ability to detect and stop threats behaviorally. It deepens the ability to detect "living-off-the-land" attacks and provides faster response to changes in the threat landscape through signature updates.

A BP event is shown in this image.

**Testing.machine2.amp** detected **Scheduled Task Containing Suspicious Target** Tactics Medium

<b>Event Overview</b>	Description		A suspicious scheduled task was created. This particular task stands out because it references a shortcut (.lnk) file. This file can create one-time only tasks, recurring tasks, and tasks that run based on specific system events, such as system startup, to establish persistence.
Connector Details	Occurred At		2022-10-20 17:07:40 UTC
Comments	<b>MITRE   ATT&amp;CK</b>	Tactics	TA0002: Execution TA0003: Persistence
		Techniques	T1053.005: Scheduled Task/Job: Scheduled Task

**Observables**

▼ File: schtasks.exe ▼ 013c013e...b0ad28ef ▼

**BP exclusion**

Process ▼	Path	Path/to/the/executable/executable.exe
Behavioral Protection	SHA	
<p>You can provide path and/or SHA-256. If you specify both a path and SHA-256, both must be met for the process to be excluded.</p> <p><input type="checkbox"/> Apply to child processes</p>		

+ Add Exclusion
+ Add Multiple Exclusions...

**Related Information**

- [For more information on the policy configuration, navigate to the User Guide](#)
- [Create Exclusions in Cisco Secure Endpoint Connector video](#)
- [Technical Support & Documentation - Cisco Systems](#)