

Uitsluitingen in Cisco Secure Endpoint Connector configureren en beheren

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Secure Endpoint-workflow](#)

[Door Cisco onderhouden uitsluitingen](#)

[Aangepaste uitsluitingen](#)

[Secure Endpoint-engine](#)

[Uitsluiting pad](#)

[Uitsluiting jokerteken](#)

[Uitsluiting bestandsuitgang](#)

[Proces: uitsluiting bestandsscan](#)

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

[Uitsluiting SPP](#)

[Bescherming tegen kwaadaardige activiteiten \(MAP\)](#)

[MAP-uitsluiting](#)

[Preventie van exploitatie \(Exprev\)](#)

[Gedragsbescherming](#)

[Gerelateerde informatie](#)

Inleiding

Dit document beschrijft hoe u de uitsluiting voor de verschillende motoren op de Cisco Secure Endpoint console kunt maken.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Een uitsluitingslijst wijzigen en toepassen op een beleid in de Secure Endpoint-console
- Windows CSIDL-conventie

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco Secure Endpoint console 5.4.20211013
- Secure Endpoint Gebruikershandleiding revisie 15 okt 2021

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Secure Endpoint-workflow

Op een hoog niveau van bewerkingen verwerkt Cisco Secure Endpoint een bestand Secure Hash Algorithm (SHA) in deze volgorde door de belangrijkste onderdelen van de connector:

- Uitsluitingen
- Tetra Engine
- Toepassingscontrole (lijst toestaan / blokkeringslijst)
- SHA Engine
- Exploitpreventie (Exprev) / Kwaadaardige Activiteit Bescherming (MAP) /
Systeemprocesbescherming / Netwerkmotor (Device Flow Correlatie)

Opmerking: de optie Uitsluiten of Toestaan/Blocklist maken is afhankelijk van de door de engine gedetecteerde bestand.

Door Cisco onderhouden uitsluitingen

Uitsluitingen voor Cisco-onderhoud worden gemaakt en onderhouden door Cisco om een betere compatibiliteit te bieden tussen de Secure Endpoint Connector en antivirus- en beveiligingsproducten of andere software.

Deze uitsluitingsstelsels bevatten verschillende soorten uitsluitingen om een goede werking te waarborgen.

U kunt de wijzigingen volgen die aan deze uitsluitingen zijn uitgevoerd in het artikel [Wijzigingen in Cisco-lijst van ondergehouden uitsluitingen voor Cisco Secure Endpoint Console](#).

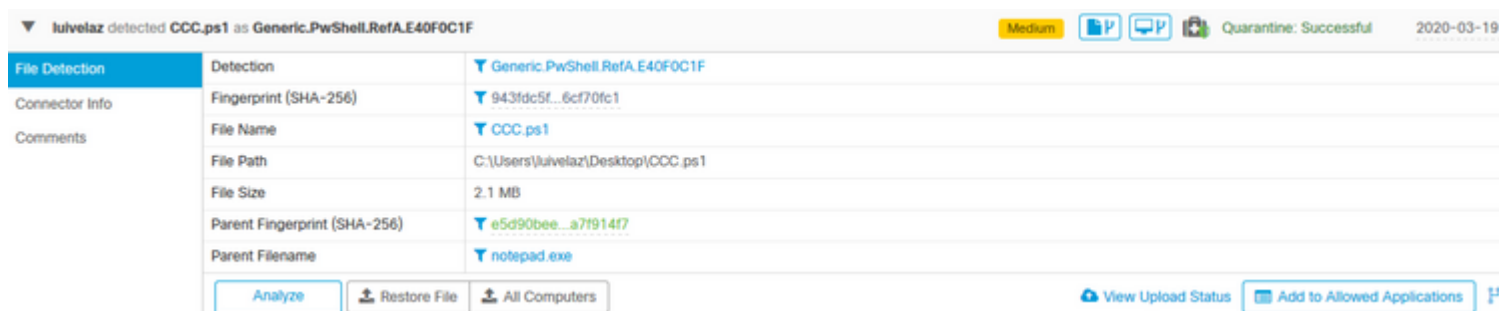
Aangepaste uitsluitingen

Secure Endpoint-engine

File Scan (CPU gebruik / bestandsdetectie) door Tetra & SHA engine:

Gebruik deze soorten uitsluitingen om detectie/quarantaine van een bestand te voorkomen of om [Secure Endpoint hoge CPU](#) te [beperken](#).

De gebeurtenis op de Secure Endpoint console is zoals in de afbeelding.



The screenshot displays a file detection event in the Cisco Secure Endpoint console. The event is titled "luivelaz detected CCC.ps1 as Generic.PwShell.RefA.E40F0C1F" with a "Medium" severity level and a "Quarantine: Successful" status. The event details are as follows:

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

At the bottom of the console, 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".

Opmerking: CSIDL kan worden gebruikt voor uitsluitingen. Raadpleeg [dit](#) Microsoft-document voor meer informatie over CSIDL.

Uitsluiting pad

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

Uitsluiting jokertekens

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

Opmerking: Optie **Toepassen op alle stationsaanduidingen** wordt ook gebruikt om de uitsluiting toe te passen op de schijven [A-Z] die aan het systeem zijn gekoppeld.

Uitsluiting bestandsuitgang

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

Waarschuwing: gebruik dit type uitsluiting met voorzichtigheid omdat het alle bestanden met de bestandsextensie uitsluit van scans, ongeacht de locatie van het pad.

Proces: uitsluiting bestandsscan

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 beschikbaar via connector versie 6.0.5 en beschermt de volgende Windows processen:

- Session Manager-subsysteem (smss.exe)
- Runtime-subsysteem client/server (csrss.exe)
- Subsysteem met lokale beveiligingsinstantie (lsass.exe)
- Windows Logon-toepassing (winlogon.exe)
- Windows Start-up-toepassing (wininit.exe)

Dit beeld toont een SPP-gebeurtenis.

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"/>		

Uitsluiting SPP

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		

Bescherming tegen kwaadaardige activiteiten (MAP)

Malicious Activity Protection (MAP) engine, verdedigt uw eindpunt tegen een ransomware aanval. Het identificeert kwaadwillige acties of processen wanneer zij uitvoeren, en beschermt uw gegevens tegen encryptie.

In deze afbeelding is een MAP-gebeurtenis afgebeeld.

Malicious Activity Protection	Fingerprint (SHA-256)	9967f55a...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)	9967f55a...2956d820
	Parent Filename	rewrite.exe
<div style="display: flex; justify-content: space-between; align-items: center;"> Analyze Restore File All Computers </div>		

MAP-uitsluiting

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		

Waarschuwing: gebruik dit soort uitsluiting voorzichtig en nadat u hebt bevestigd dat de detectie inderdaad niet kwaadaardig is.

Preventie van exploitatie (Exprev)

De exploit prevention engine verdedigt uw endpoints tegen geheugeninjecties die vaak worden gebruikt door malware en andere zero-day aanvallen op niet-gepatcheerde software kwetsbaarheden. Wanneer het een aanval tegen een beschermd proces ontdekt zal het worden geblokkeerd en een gebeurtenis genereren, maar er zal geen quarantaine zijn.

In deze afbeelding wordt een gebeurtenis Exprev weergegeven.

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-uitsluiting

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...

Waarschuwing: gebruik deze uitsluiting wanneer u de activiteit op de betreffende module/toepassing vertrouwt.

Gedragsbescherming

De behavioral protection engine vergroot de mogelijkheid om bedreigingen op gedragswijze te detecteren en te stoppen. Het vergroot de mogelijkheid om aanvallen op andere gebieden dan het land te detecteren en biedt snellere reactie op veranderingen in het bedreigingslandschap door handtekeningupdates.

In deze afbeelding wordt een bloeddrukgebeurtenis weergegeven.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.