

# Configuration et gestion des exclusions dans Cisco Secure Endpoint Connector

## Table des matières

---

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Workflow Secure Endpoint](#)

[Exclusions maintenues par Cisco](#)

[Exclusions personnalisées](#)

[Moteur Secure Endpoint](#)

[Exclusion du chemin](#)

[Exclusion générique](#)

[Exclusion des extensions de fichier](#)

[Processus : Exclusion de l'analyse des fichiers](#)

[Protection des processus système \(SPP\)](#)

[Exclusion SPP](#)

[Protection contre les activités malveillantes \(MAP\)](#)

[Exclusion MAP](#)

[Prévention des exploits \(Exprev\)](#)

[Protection du comportement \(BP\)](#)

[Informations connexes](#)

---

## Introduction

Ce document décrit comment créer l'exclusion pour les différents moteurs sur la console Cisco Secure Endpoint.

## Conditions préalables

### Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Modifier et appliquer une liste d'exclusion à une stratégie dans la console Secure Endpoint
- convention CSIDL de Windows

### Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Console Cisco Secure Endpoint 5.4.20211013
- Révision du guide de l'utilisateur Secure Endpoint le 15 octobre 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. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

## Workflow Secure Endpoint

Dans un haut niveau d'opérations, le point d'extrémité sécurisé Cisco traite un fichier SHA (Secure Hash Algorithm) dans cet ordre via les principaux composants du connecteur :

- Exclusions
- Moteur Tetra
- Contrôle des applications (liste verte/liste de blocage)
- Moteur SHA
- Prévention des exploits (Exprev) / Protection contre les activités malveillantes (MAP) / Protection des processus système / Moteur réseau (corrélation des flux de périphériques)

---

 Remarque : l'exclusion ou la création d'une liste verte ou de blocage dépend du moteur qui a détecté le fichier.

---

## Exclusions maintenues par Cisco

Les exclusions maintenues par Cisco sont créées et maintenues par Cisco afin d'assurer une meilleure compatibilité entre le connecteur Secure Endpoint et l'antivirus, les produits de sécurité ou d'autres logiciels.

Ces jeux d'exclusions contiennent différents types d'exclusions pour garantir un fonctionnement correct.

Vous pouvez suivre les modifications apportées à ces exclusions dans l'article [Modifications de la liste d'exclusion de Cisco pour Cisco Secure Endpoint Console](#).

## Exclusions personnalisées

### Moteur Secure Endpoint


Analyse de fichiers (utilisation CPU / détections de fichiers) par Tetra & moteur SHA :

Utilisez ces types d'exclusions pour éviter la détection/la mise en quarantaine d'un fichier ou pour [réduire le niveau élevé de CPU du point de terminaison sécurisé](#).

L'événement sur la console Secure Endpoint est illustré dans l'image.

luivelaz detected CCC.ps1 as Generic.PwShell.RefA.E40F0C1F Medium    Quarantine: Successful 2020-03-19 23:19:11 UTC

|                |                              |                                   |
|----------------|------------------------------|-----------------------------------|
| File Detection | Detection                    | Generic.PwShell.RefA.E40F0C1F     |
| Connector Info | Fingerprint (SHA-256)        | 943fdc5f...6cf70fc1               |
| Comments       | 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                       |


 Remarque : CSIDL peut être utilisé pour les exclusions. Consultez [ce](#) document Microsoft pour plus d'informations sur CSIDL.

### Exclusion du chemin

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


### Exclusion générique

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


 Remarque : l'option Apply to all drive letters est utilisée pour appliquer également l'exclusion aux lecteurs [A-Z] connectés au système.

### Exclusion des extensions de fichier

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

 Attention : utilisez ce type d'exclusion avec précaution car il exclut tous les fichiers portant l'extension de fichier des analyses, quel que soit l'emplacement du chemin d'accès.

### Processus : Exclusion de l'analyse des fichiers

|           |  |                           |   |
|-----------|--|---------------------------|---|
| 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   |                           |   |

### Protection des processus système (SPP)

Le moteur System Process Protection est disponible à partir de la version 6.0.5 du connecteur et protège les processus Windows suivants :

- Sous-système Gestionnaire de session (smss.exe)
- Sous-système d'exécution client/serveur (csrss.exe)
- Sous-système de l'autorité de sécurité locale (lsass.exe)
- Application de connexion Windows (winlogon.exe)
- Application de démarrage Windows (wininit.exe)

Cette image présente un événement SPP.

▼ UMONTERO-Y36YQ.cisco.com prevented unexpected access to lsass.exe by TestAMPprotect.exe. Low [P] [P] [P] System Process Protection 2020-03-09 21:03:11 UTC

|                |                              |  |
|----------------|------------------------------|--|
| 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                                    |

[Analyze](#)

## Exclusion 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 conditions must 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 conditions must be met for the process to be excluded. |      |  |
| <input checked="" type="checkbox"/> Apply to child processes   |      |  |

## Protection contre les activités malveillantes (MAP)


Le moteur de protection contre les activités malveillantes (MAP) protège votre terminal d'une attaque par ransomware. Il identifie les actions ou les processus malveillants lors de leur exécution et protège vos données contre le chiffrement.

Un événement MAP est illustré dans cette image.

|  |                              |  |
|--|------------------------------|--|
| 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<br>C:\Users\umontero\Desktop\Test files\AMP4E-8120-SPP-MAP-EXPREV-test_files\Map\rewrite_data\0.txt.new<br>C:\Users\umontero\Desktop\Test files\AMP4E-8120-SPP-MAP-EXPREV-test_files\Map\rewrite_data\4.txt.new<br>C:\Users\umontero\Desktop\Test files\AMP4E-8120-SPP-MAP-EXPREV-test_files\Map\rewrite_data\2.txt.new<br>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; gap: 10px;"> <span>Analyze</span> <span>Restore File</span> <span>All Computers</span> </div> |                              |  |

## Exclusion MAP

|   |      |                            |
|---|------|----------------------------|
| 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> <p><input checked="" type="checkbox"/> Apply to child processes</p> |      |                            |

 Attention : utilisez ce type d'exclusion avec précaution et après avoir confirmé que la détection n'est pas malveillante.

## Prévention des exploits (Exprev)

Le moteur de prévention des exploits protège vos terminaux des attaques par injection de mémoire couramment utilisées par les programmes malveillants et d'autres attaques de type « zero-day » sur des logiciels non corrigés vulnérabilités. Lorsqu'il détecte une attaque contre un processus protégé, il est bloqué et génère un événement, mais il n'y a pas de quarantaine.

Un événement Exprev est affiché dans cette 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\lend...app_1d4e2229d1ba886_07e5.0402_a608579ft |
|  | File Size                    | 5.82 MB  |
|  | Parent Fingerprint (SHA-256) | 375a7501...e8624659  |
|  | Parent Filename              | dfsvc.exe  |
|  | Parent File Size             | 24.27 KB   |
| <div style="display: flex; gap: 10px;"> <span>Analyze</span> </div>    |                              |  |

## Exclusion Exprev

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

Attention : utilisez cette exclusion chaque fois que vous approuvez l'activité sur le module/l'application affecté(e).

## Protection du comportement (BP)

Le moteur de protection comportementale améliore la capacité de détection et d'arrêt comportemental des menaces. Il renforce la capacité à détecter les attaques « hors du pays » et fournit une réponse plus rapide aux changements dans le paysage des menaces grâce à des mises à jour des signatures.

Un événement BP est illustré dans cette image.

Testing.machine2.amp detected Scheduled Task Containing Suspicious Target Tactics ●●●●●●●● Medium Threat Detection 2022-10-20 17:07:41 UTC

|                       |   |   |         |                                       |            |   |
|-----------------------|---|---|---------|---------------------------------------|------------|---|
| <b>Event Overview</b> | Description                                   | A suspicious scheduled task was created. This particular task stands out because it references a shortcut (.lnk) or a VB script file (.vba or .vbs). The schtasks command can create one-time only tasks, recurring tasks, and tasks that run based on specific system events, such as logon and startup. Malware can use scheduled tasks to establish persistence. |         |                                       |            |   |
| Connector Details     | Occured At                                    | 2022-10-20 17:07:40 UTC   |         |                                       |            |   |
| Comments              | MITRE ATT&CK                                  | <table border="1"> <tr> <td>Tactics</td> <td>TA0002: Execution TA0003: Persistence</td> </tr> <tr> <td>Techniques</td> <td>T1053.005: Scheduled Task/Job: Scheduled Task</td> </tr> </table>  | Tactics | TA0002: Execution TA0003: Persistence | Techniques | T1053.005: Scheduled Task/Job: Scheduled Task |
| Tactics               | TA0002: Execution TA0003: Persistence         |   |         |                                       |            |   |
| Techniques            | T1053.005: Scheduled Task/Job: Scheduled Task |   |         |                                       |            |   |

**Observables**

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

## exclusion des points de présence

|   |      |  |  |
|---|------|--|--|
| Process   | Path | Path/to/the/executable/executable.exe  |  |
| Behavioral Protection                             | 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 type="checkbox"/> Apply to child processes |      |  |  |

## Informations connexes

- [Pour plus d'informations sur la configuration des politiques, accédez au Guide de l'utilisateur](#)
- [Créer des exclusions dans la vidéo Cisco Secure Endpoint Connector](#)

- [Assistance et documentation techniques - Cisco Systems](#)

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.