Configuración e identificación de exclusiones de terminales seguros

Contenido

Introducción

Este documento describe qué son las exclusiones, cómo identificarlas y las prácticas recomendadas para crear exclusiones en Cisco Secure Endpoint.

Descargo

La información de este documento se basa en los sistemas operativos Windows, Linux y macOS.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Overview

Después de leer este documento, debe entender:

- Qué es una exclusión y los diferentes tipos de exclusiones disponibles para Cisco Secure Endpoint.
- Cómo preparar el conector para el ajuste de exclusión.
- Cómo identificar exclusiones potencialmente fuertes.
- Cómo crear nuevas exclusiones en Cisco Secure Endpoint Console.
- Cuáles son las prácticas recomendadas para crear exclusiones.

¿Qué son las exclusiones?

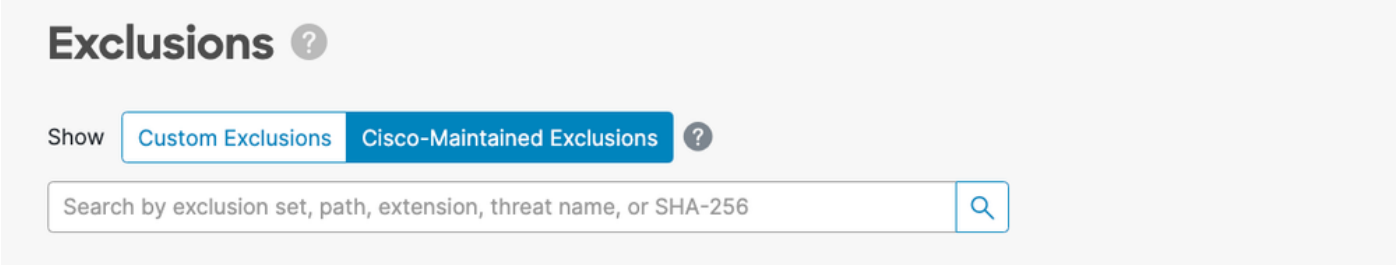
Un conjunto de exclusiones es una lista de directorios, extensiones de archivos, rutas de acceso a archivos, procesos, nombres de amenazas, aplicaciones o indicadores de riesgo que no desea que el conector analice o confirme. Las exclusiones deben diseñarse cuidadosamente para garantizar un equilibrio entre el rendimiento y la seguridad en un equipo cuando se habilita la protección de terminales, como un terminal seguro. En este artículo se describen las exclusiones de Secure Endpoint Cloud, TETRA, SPP y MAP.

Cada entorno es único, así como la entidad que lo controla, que varía desde políticas estrictas a políticas abiertas. Como tal, las exclusiones deben adaptarse exclusivamente a cada situación.

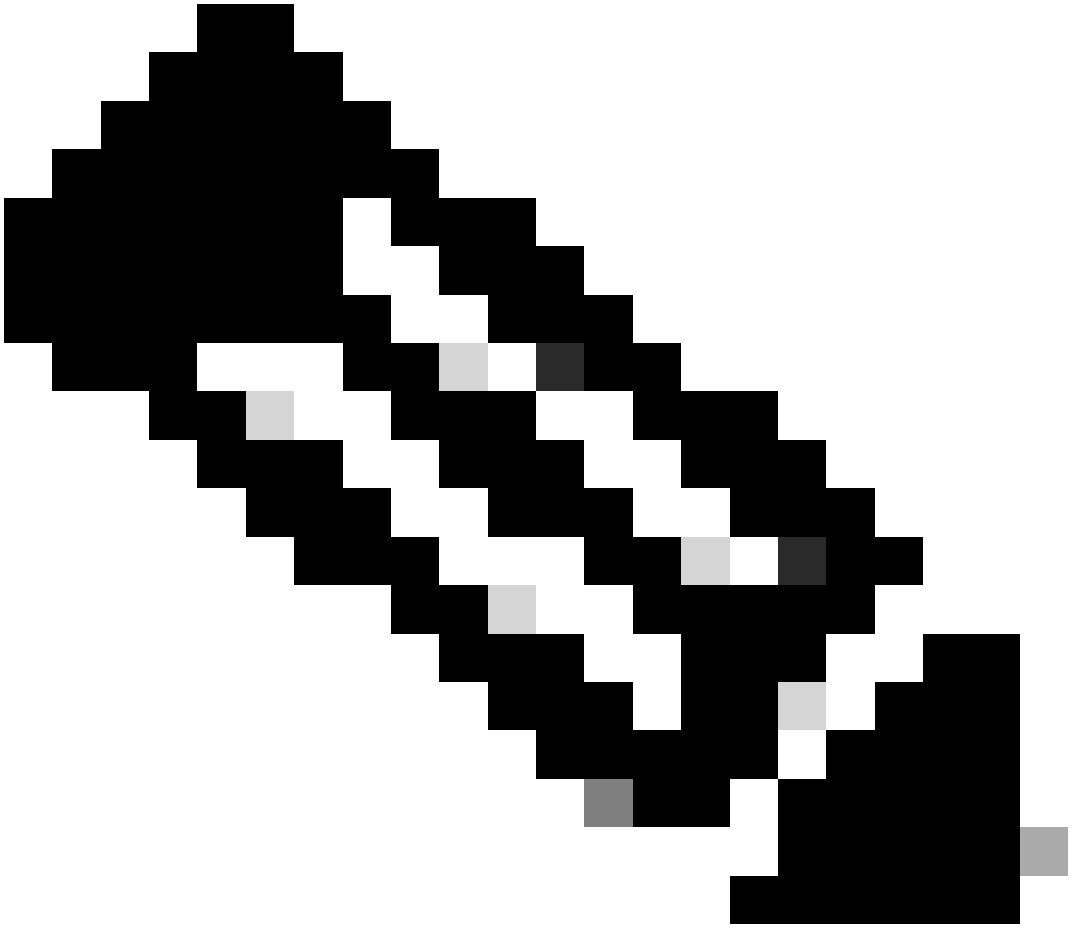
Las exclusiones se pueden clasificar de dos formas: exclusiones mantenidas por Cisco y exclusiones personalizadas.

Exclusiones mantenidas por Cisco

Las exclusiones mantenidas por Cisco son exclusiones que se han creado a partir de investigaciones y que se han sometido a rigurosas pruebas en sistemas operativos, programas y otro software de seguridad de uso común. Estas exclusiones se pueden visualizar seleccionando `Exclusiones Mantenidas por Cisco` en Secure Endpoint Console en la página `Exclusiones`.



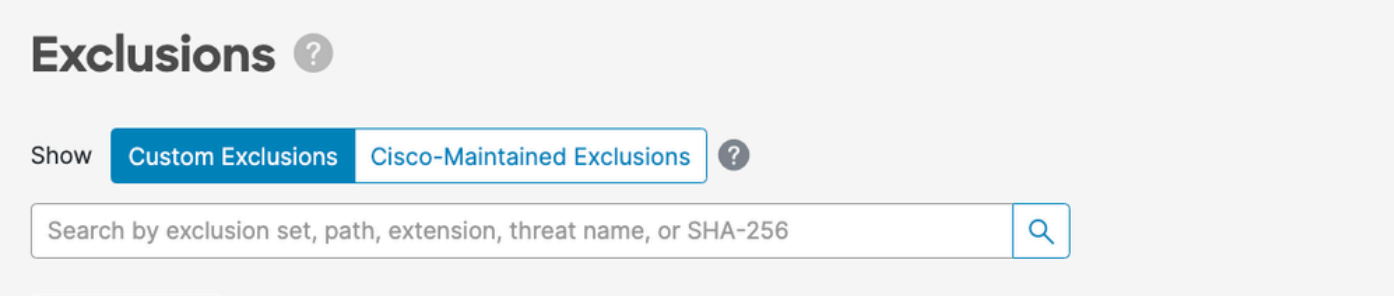
Cisco supervisa las listas de exclusión recomendadas publicadas por los proveedores de antivirus y actualiza las exclusiones mantenidas por Cisco para incluir las exclusiones recomendadas.



> Nota: es posible que algunos proveedores de antivirus no publiquen sus exclusiones recomendadas. En este caso, es posible que el cliente tenga que ponerse en contacto con el proveedor de antivirus para solicitar una lista de exclusiones recomendadas y, a continuación, abrir un caso de asistencia para actualizar las exclusiones mantenidas por Cisco.

Exclusiones personalizadas

Las exclusiones personalizadas son exclusiones que ha creado un usuario para un caso práctico personalizado en un terminal. Estas exclusiones se pueden visualizar seleccionando `Custom Exclusions` en Secure Endpoint Console en la página `Exclusions`.



Tipos de exclusiones

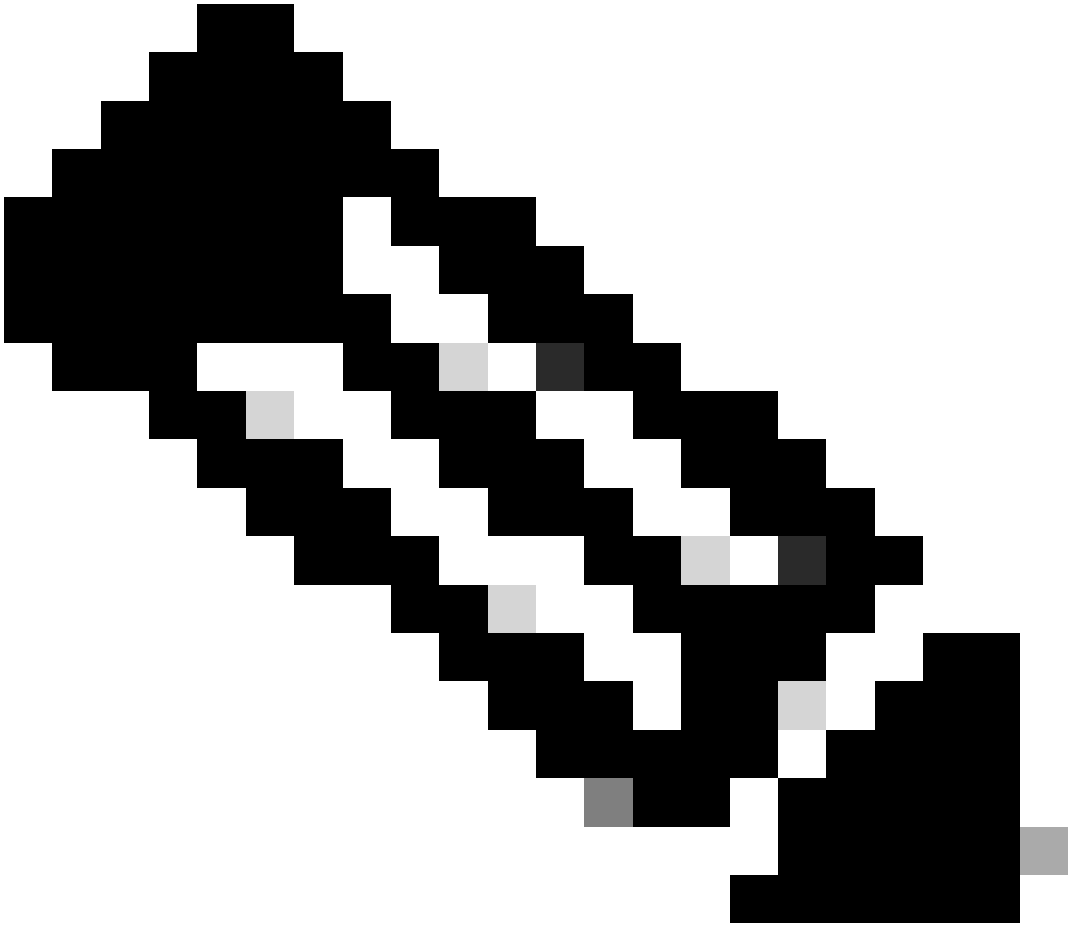
Exclusiones de procesos

Las exclusiones de procesos permiten a los administradores excluir procesos de los motores admitidos. Los motores que admiten exclusiones de procesos en cada plataforma se describen en la siguiente tabla:

Sistema operativo	Motor			
	Análisis de archivos	Protección de procesos del sistema	Protección de actividad maliciosa	Protección del comportamiento
Windows:	✓	✓	✓	✓
Linux	✓	✗	✗	✓
macOS	✓	✗	✗	✓

MacOS y Linux

Debe proporcionar una ruta de acceso absoluta al crear una exclusión de proceso; también puede proporcionar un usuario opcional. Si especifica una ruta y un usuario, se deben cumplir ambas condiciones para excluir el proceso. Si no especifica un usuario, la exclusión de proceso se aplicará a todos los usuarios.



Nota: En macOS y Linux, las exclusiones de procesos se aplican a todos los motores.

Caracteres comodín de proceso:

Los conectores Secure Endpoint Linux y macOS admiten el uso de un comodín en la exclusión de procesos. Esto permite una cobertura más amplia con menos exclusiones, pero también puede ser peligroso si se deja demasiado sin definir. Sólo debe utilizar el carácter comodín para cubrir el número mínimo de caracteres necesarios para proporcionar la exclusión necesaria.

Uso del comodín de proceso para macOS y Linux:

- El carácter comodín se representa mediante un único carácter de asterisco (*)
- El comodín se puede utilizar en lugar de un solo carácter o un directorio completo.
- La colocación del carácter comodín al principio de la ruta se considera no válida.
- El carácter comodín funciona entre dos caracteres definidos, barras diagonales o caracteres alfanuméricos.

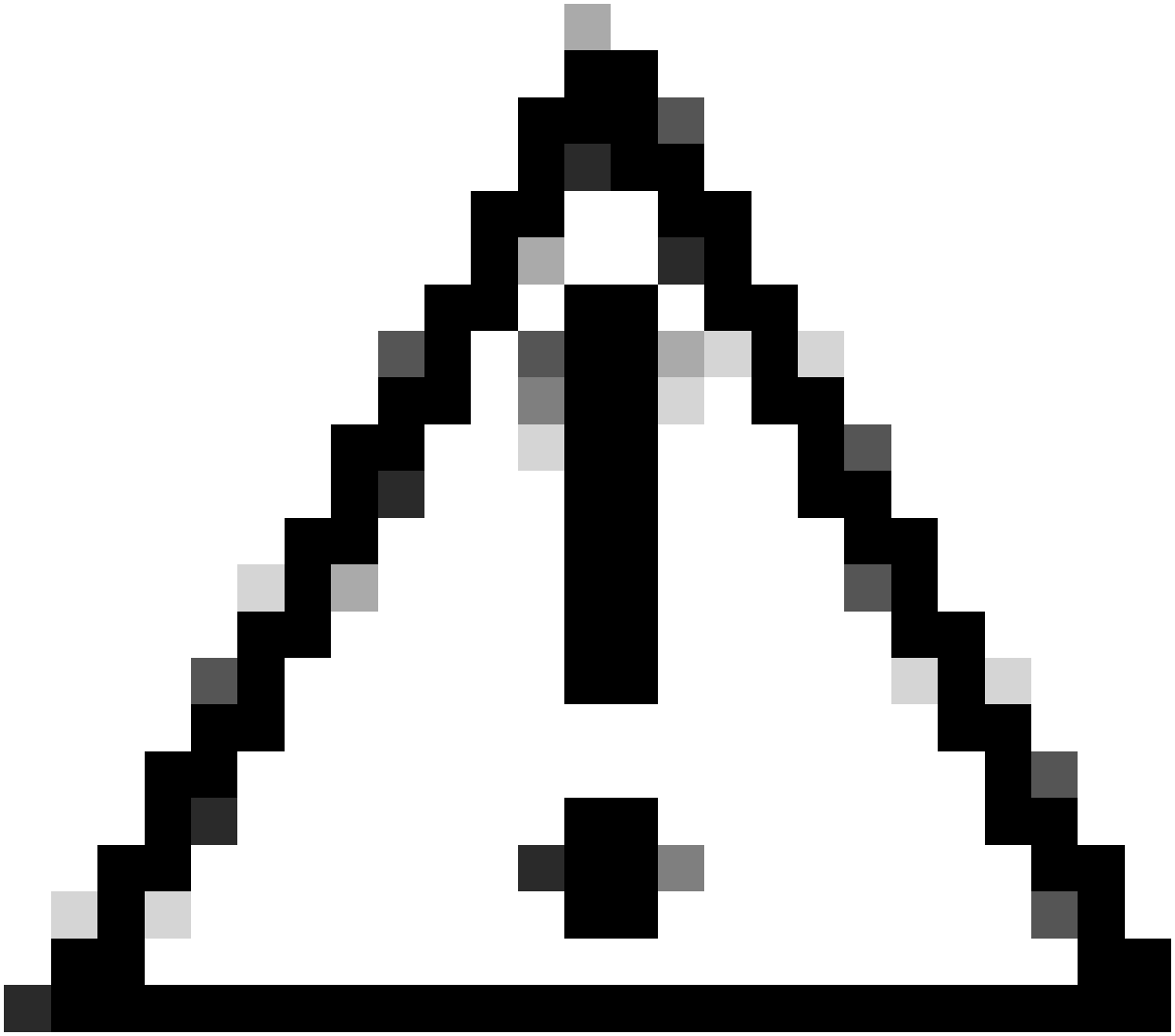
Examples:

Exclusión	Resultado esperado
`/Library/Java/JavaVirtualMachines/*/java`	Excluye `Java` en todas las subcarpetas de `JavaVirtualMachines`
`/Library/Jibber/j*bber`	Excluye el proceso para `jabber`, `jibber`, `jobber`, etc

Windows:

Puede proporcionar una ruta de acceso absoluta y/o un SHA-256 del proceso ejecutable al crear una exclusión de proceso. Si especifica una ruta de acceso y SHA-256, se deben cumplir ambas condiciones para que se excluya el proceso.

En Windows, también puede utilizar CSIDL o KNOWNFOLDERID en la ruta de acceso para crear exclusiones de procesos.

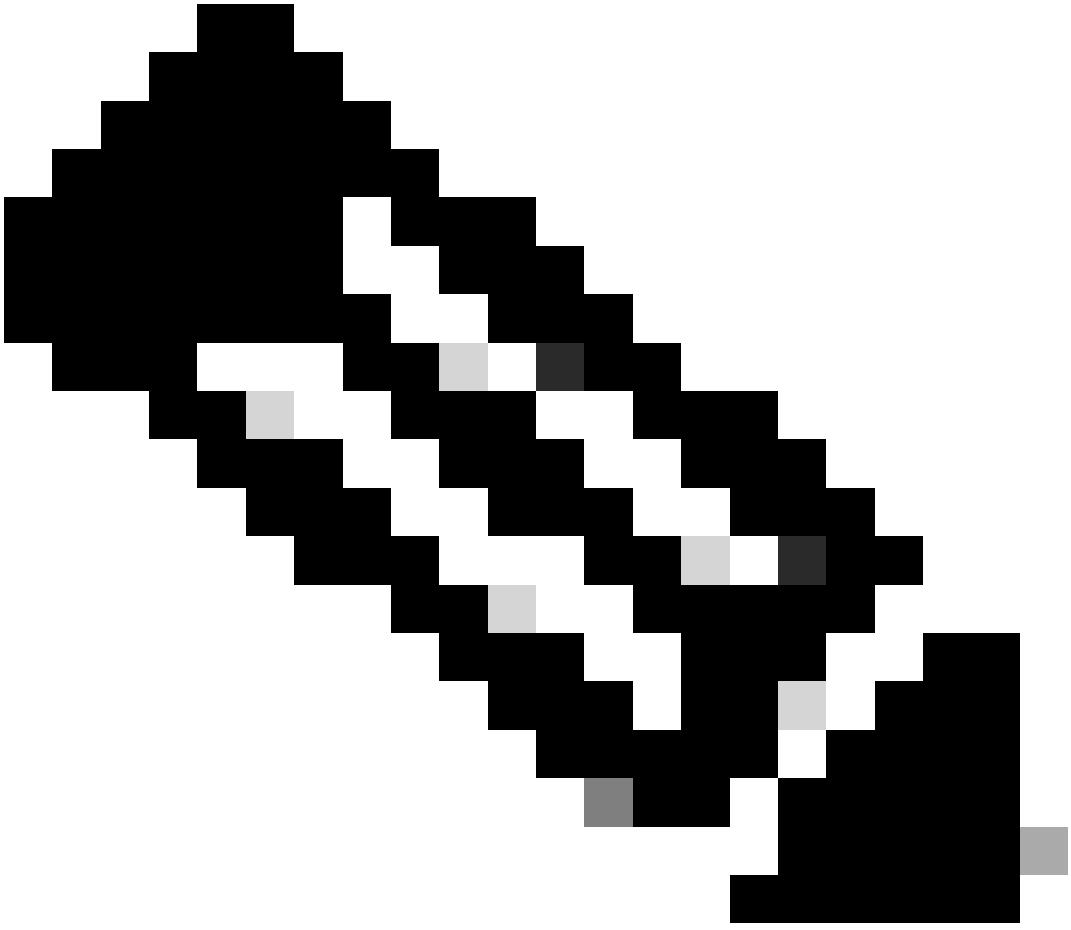


Precaución: Los procesos secundarios creados por un proceso excluido no se excluyen por defecto. Para excluir procesos adicionales al crear una exclusión de procesos, `seleccione Aplicar a procesos secundarios.`

Limitaciones:

- Si el tamaño del archivo del proceso es mayor que el tamaño máximo del archivo de análisis establecido en la directiva, el SHA-256 del proceso no se calculará y la exclusión no funcionará. Utilice una exclusión de proceso basada en ruta para archivos mayores que el tamaño máximo del archivo de análisis.
- El conector de Windows impone un límite de 500 exclusiones de procesos en todos los tipos de exclusión de procesos.
    - Las exclusiones de procesos sólo se respetan hasta el límite, empezando por la parte superior de la lista de exclusiones de procesos en `policy.xml`.
    - Todas las directivas de Windows tienen una exclusión de procesos para `sfc.exe`, que se descuenta del límite de exclusiones de procesos:

      ```
      <item>3|0||CSIDL_Secure Endpoint_VERSION\sfc.exe|48|</item>
      ```



Nota: En Windows, las exclusiones de procesos se aplican por motor. Si la misma exclusión se debe aplicar a varios motores, la exclusión de proceso se debe duplicar en

---

este caso para cada motor aplicable.

Caracteres comodín de proceso:

Los conectores de Windows de terminal seguro admiten el uso de un comodín en la exclusión de procesos. Esto permite una cobertura más amplia con menos exclusiones, pero también puede ser peligroso si se deja demasiado sin definir. Sólo debe utilizar el carácter comodín para cubrir el número mínimo de caracteres necesarios para proporcionar la exclusión necesaria.

Uso del comodín de proceso para Windows:

- El carácter comodín se representa mediante un único carácter de asterisco () y un doble asterisco (*)
- Comodín de asterisco único (*):
  - El comodín se puede utilizar en lugar de un solo carácter o un directorio completo.
  - La colocación del carácter comodín al principio de la ruta se considera no válida.
  - El carácter comodín funciona entre dos caracteres definidos, barras diagonales o caracteres alfanuméricos.
  - Al colocar el carácter comodín al final de una ruta de acceso se excluyen todos los procesos de ese directorio, pero no los subdirectorios.
- Comodín de asterisco doble (**):
  - Sólo se puede colocar al final de un trazado.
  - Al colocar el carácter comodín al final de una ruta de acceso se excluyen todos los procesos de ese directorio y todos los procesos de los subdirectorios.
  - Esto permite un conjunto de exclusión mucho mayor con una entrada mínima, pero también deja un gran agujero de seguridad para la visibilidad. Utilice esta función con extrema precaución.

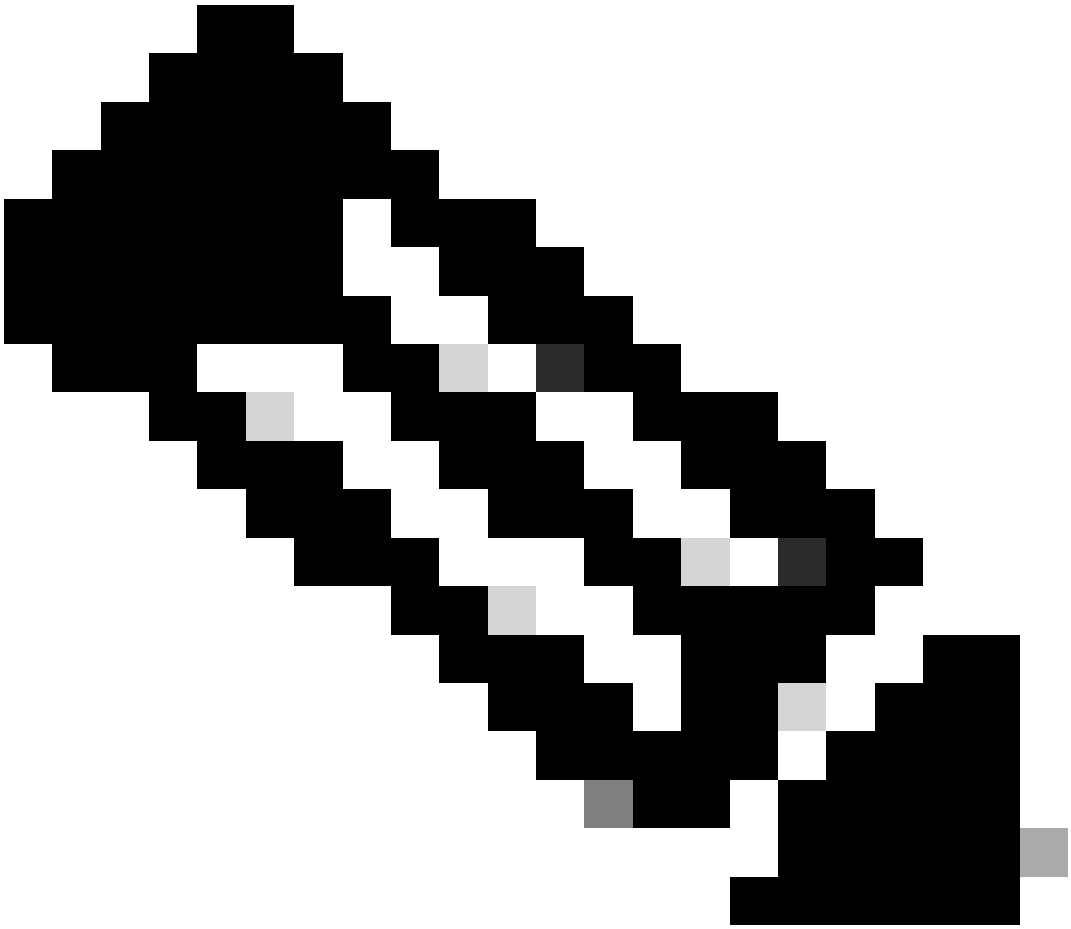
Examples:

Exclusión	Resultado esperado
`C:\Windows\*\Tiworker.exe`	Excluye todos los procesos `Tiworker.exe` encontrados en los subdirectorios de `Windows`
`C:\Windows\P*t.exe`	Excluye `Pot.exe`, `Pat.exe`, `P1t.exe`, etc
`C:\Windows\*pollos.exe`	Excluye todos los procesos del directorio de `Windows` que terminan en `pollos.exe`
`C:\*`	Excluye todos los procesos de la unidad `C:` pero no de los subdirectorios
`C:\**`	Excluye todos los procesos de la unidad `C:`

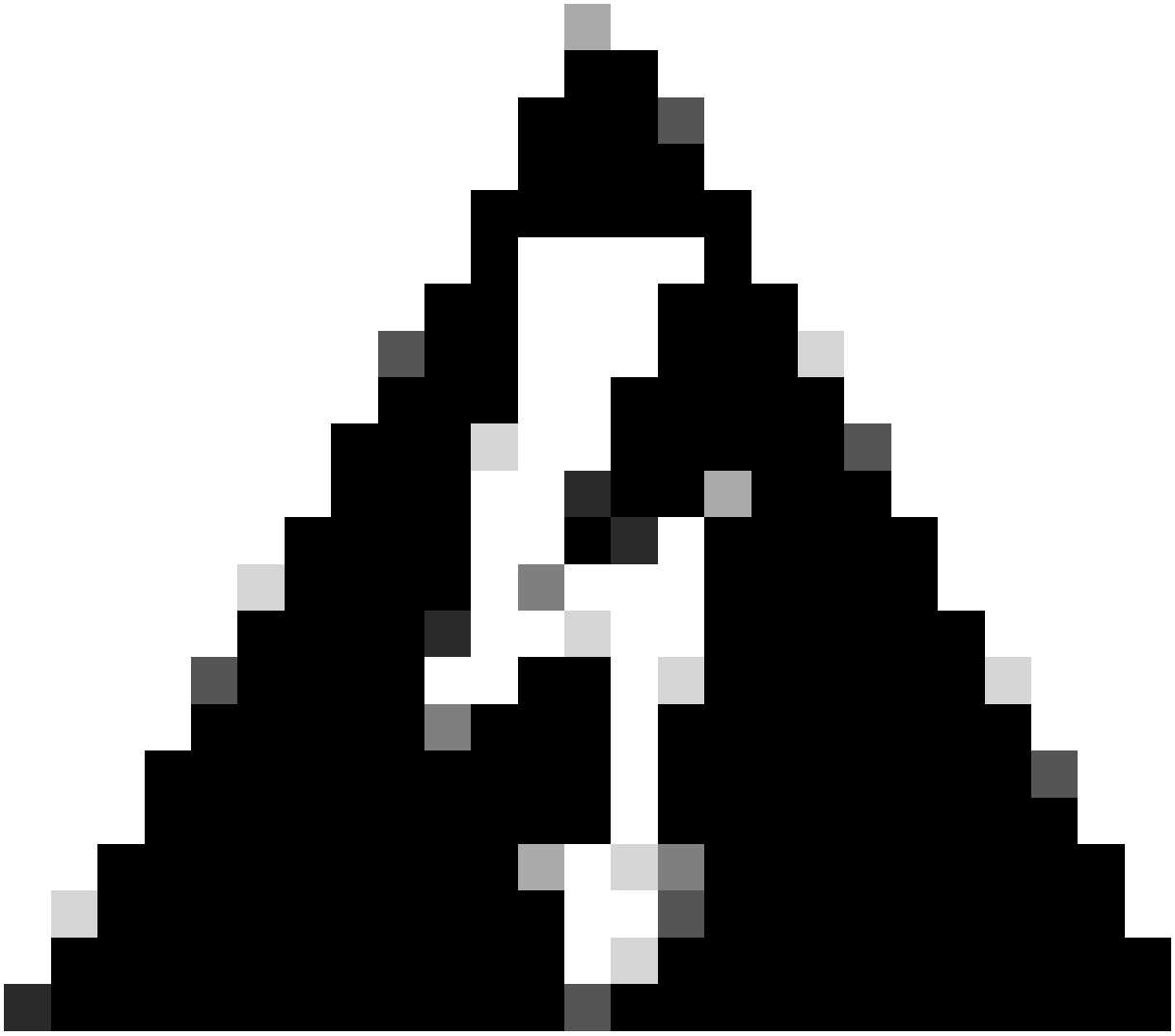
Exclusiones de amenazas

Las exclusiones de amenazas le permiten excluir un nombre de amenaza concreto de la activación de eventos. Sólo debe utilizar una exclusión de amenaza si está seguro de que los eventos son el resultado de una detección de falsos positivos. En este caso, utilice el nombre

exacto de la amenaza del evento como exclusión de la amenaza. Tenga en cuenta que, si utiliza este tipo de exclusión, ni siquiera se detectará, pondrá en cuarentena o generará un evento una detección realmente positiva del nombre de la amenaza.



Nota: las exclusiones de amenazas no distinguen entre mayúsculas y minúsculas. Ejemplo:`W32.Zombies.NotAVirus y w32.zombies.notavirus` coinciden con el mismo nombre de amenaza.



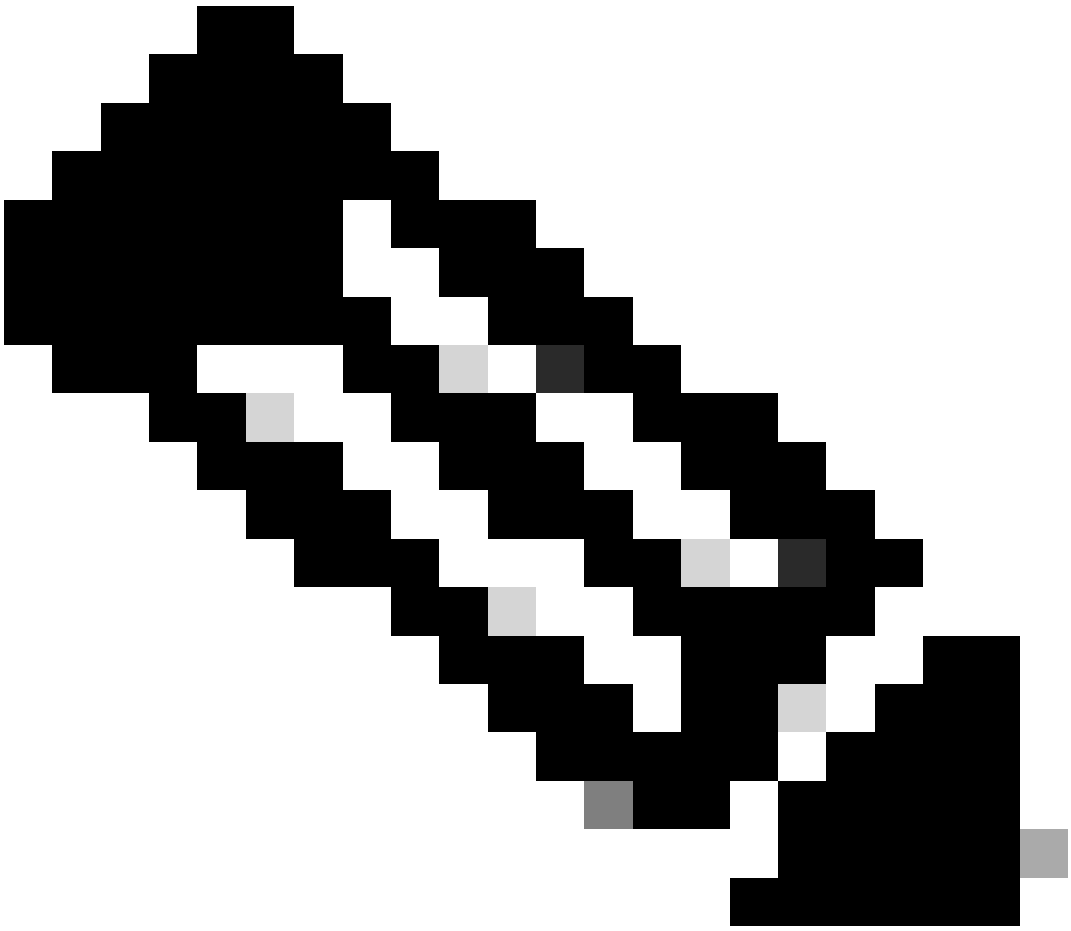
> Advertencia: no excluya las amenazas a menos que una investigación exhaustiva haya confirmado que el nombre de la amenaza es falso positivo. Las amenazas excluidas ya no se incluyen en la ficha de eventos para su revisión y auditoría.

Exclusiones de rutas

Las exclusiones de rutas de acceso son las más utilizadas, ya que los conflictos de aplicaciones suelen implicar la exclusión de un directorio. Puede crear una exclusión de ruta mediante una ruta absoluta. En Windows, también puede utilizar CSIDIL o KNOWNFOLDERID para crear exclusiones de ruta.

Por ejemplo, para excluir una aplicación AV en el directorio `Archivos de programa` de Windows, la ruta de exclusión podría ser cualquiera de las siguientes:

```
C:\Program Files\MyAntivirusAppDirectory
CSIDL_PROGRAM_FILES\MyAntivirusAppDirectory
FOLDERID_ProgramFiles\MyAntivirusAppDirectory
```



Nota: Las exclusiones de rutas son recursivas y excluyen también todos los subdirectorios.

Coincidencias parciales de ruta (sólo para Windows)

Si no se proporciona una barra diagonal final en la exclusión Path, el conector de Windows realiza una coincidencia parcial en las rutas. Mac y Linux no admiten coincidencias de ruta parciales.

Por ejemplo, si aplica las siguientes exclusiones Path en Windows:

```
C:\Program Files
C:\test
```

A continuación, se excluirán todas las rutas siguientes:

```
C:\Program Files
C:\Program Files (x86)
C:\test
C:\test123
```

Si cambia la exclusión de `"C:\test"` a `"C:\test\"`, evitará que `"C:\test123"` se excluya.

Exclusiones de extensiones de archivo

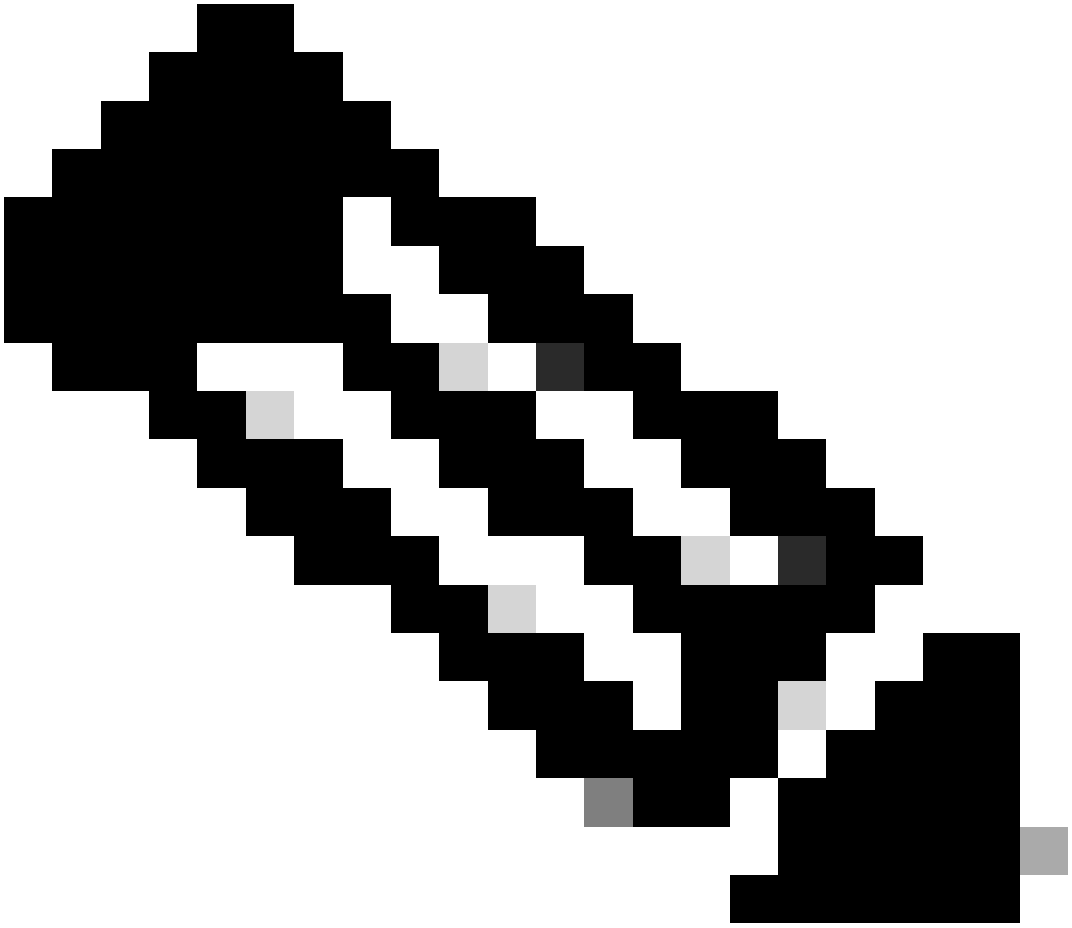
Las exclusiones de la extensión de archivo permiten la exclusión de todos los archivos con una extensión determinada.

Puntos clave:

- La entrada esperada en Secure Endpoint Console es `.extension`
- Secure Endpoint Console antepone automáticamente un punto a la extensión del archivo si no se ha agregado ninguno.
- Las extensiones no distinguen entre mayúsculas y minúsculas.

Por ejemplo, para excluir todos los archivos de base de datos de Microsoft Access, puede crear la siguiente exclusión:

```
.MDB
```



Nota: Las exclusiones de extensiones de archivo estándar están disponibles en la lista predeterminada; no se recomienda eliminar estas exclusiones, ya que esto puede provocar cambios de rendimiento en el terminal.

Exclusiones de comodines

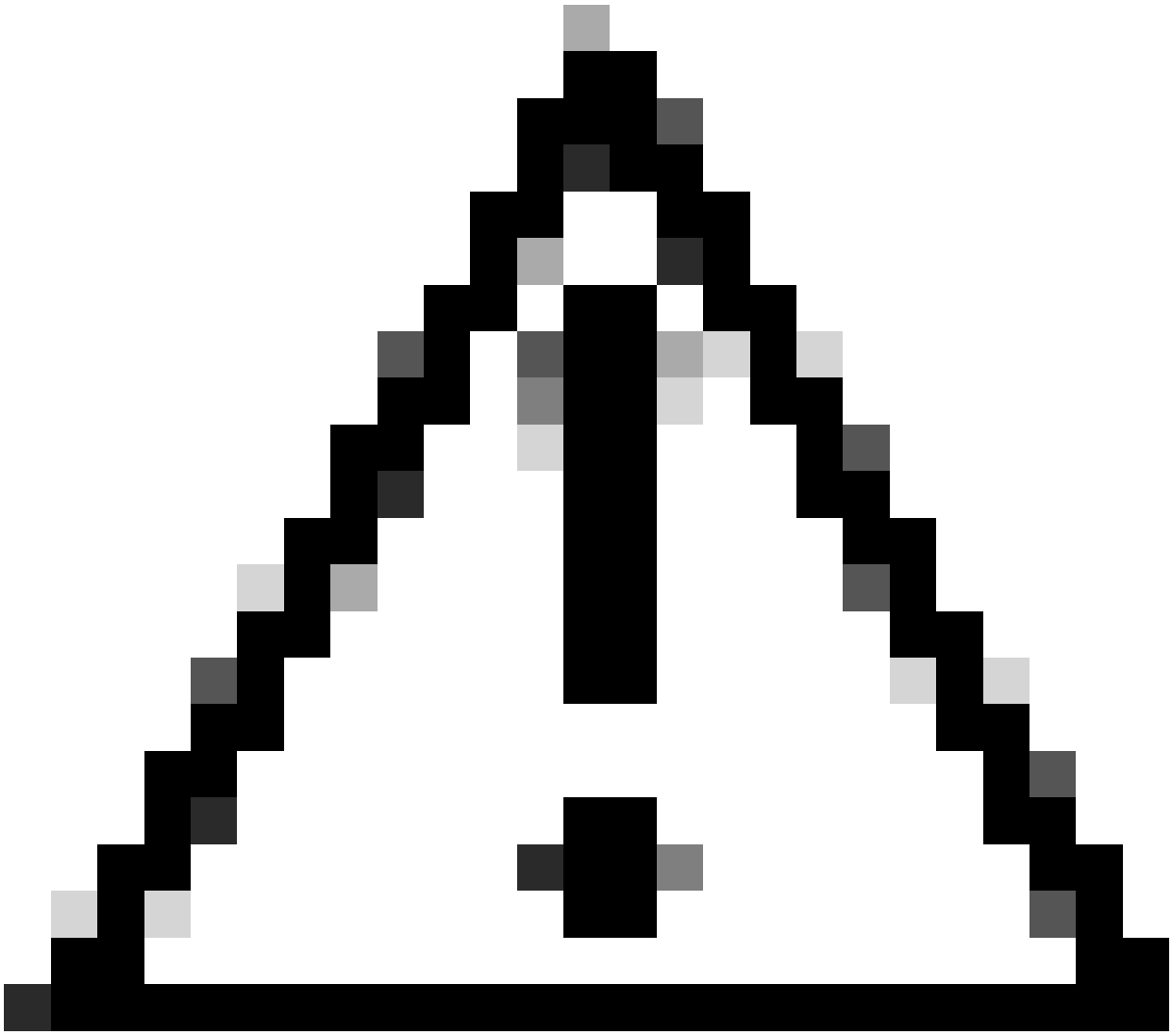
Las exclusiones de comodines son iguales a las exclusiones de ruta de acceso o extensión de archivo, excepto en que puede utilizar un carácter de asterisco (*) para representar un comodín en la ruta de acceso o extensión.

Por ejemplo, si desea excluir las máquinas virtuales de macOS de la exploración, puede introducir esta exclusión de ruta:

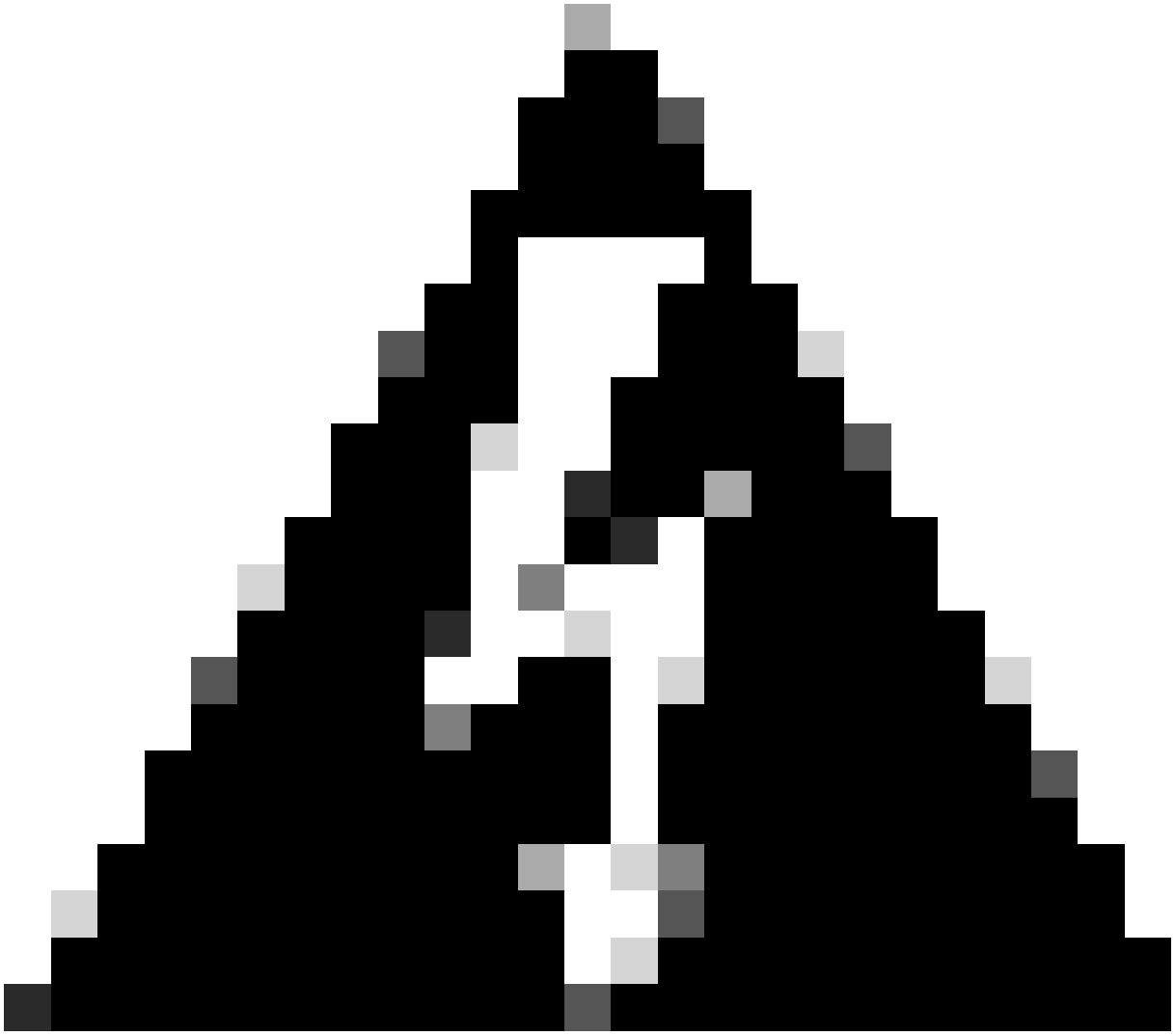
```
/Users/johndoe/Documents/Virtual Machines/
```

Sin embargo, esta exclusión sólo funcionará para un usuario, por lo que en su lugar reemplace el nombre de usuario en la ruta con un asterisco y cree una exclusión de comodín en su lugar para excluir este directorio para todos los usuarios:

```
/Users/*/Documents/Virtual Machines/
```



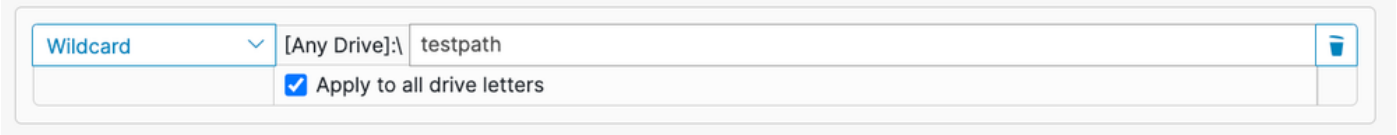
Precaución: las exclusiones de comodines no se detienen en los separadores de rutas, lo que puede dar lugar a exclusiones no deseadas. Por `ejemploC:\*\test` excluyeC:\sample\test así como `C:\1\test** oC:\sample\test123`.



> Advertencia: el inicio de una exclusión con un carácter de asterisco puede causar problemas de rendimiento importantes. Elimine o cambie todas las exclusiones que comiencen con un carácter de asterisco para mitigar el impacto en la CPU.

Windows:

Al crear exclusiones de comodines en Windows, existe la opción `Aplicar a todas las letras de unidad`. Al seleccionar esta opción, se aplica la exclusión de comodines a todas las unidades montadas.



Si tuviera que elaborar manualmente la misma exclusión, tendría que anteponerla a `^[A-Za-z]`, por ejemplo:

```
^[A-Za-z]\testpath
```

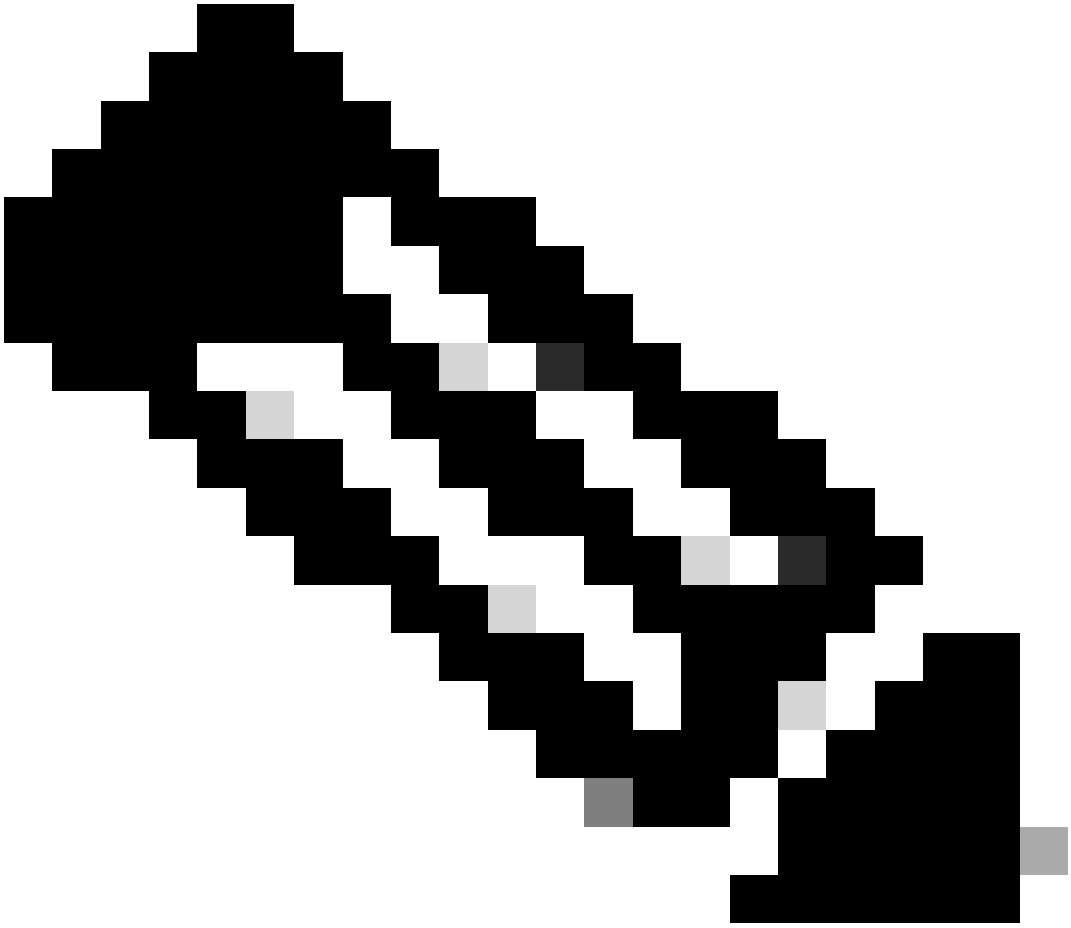
En ambos ejemplos, se excluirán C:\testpath y D:\testpath.

Secure Endpoint Console genera automáticamente el símbolo `^[A-Za-z]` cuando se selecciona `Aplicar a todas las letras de unidad` para las exclusiones de comodines.

Exclusiones ejecutables (sólo para Windows)

Las exclusiones ejecutables sólo se aplican a los conectores de Windows con la prevención de exploits habilitada. Una exclusión de archivo ejecutable impide que determinados archivos ejecutables estén protegidos por la prevención de vulnerabilidades. Sólo debe excluir un ejecutable de la prevención de vulnerabilidades si tiene problemas o problemas de rendimiento.

Puede comprobar la lista de procesos protegidos y excluir cualquier elemento de la protección especificando su nombre ejecutable en el campo de exclusión de la aplicación. Las exclusiones ejecutables deben coincidir exactamente con el nombre del archivo ejecutable con el formato `name.exe`. No se admiten comodines.

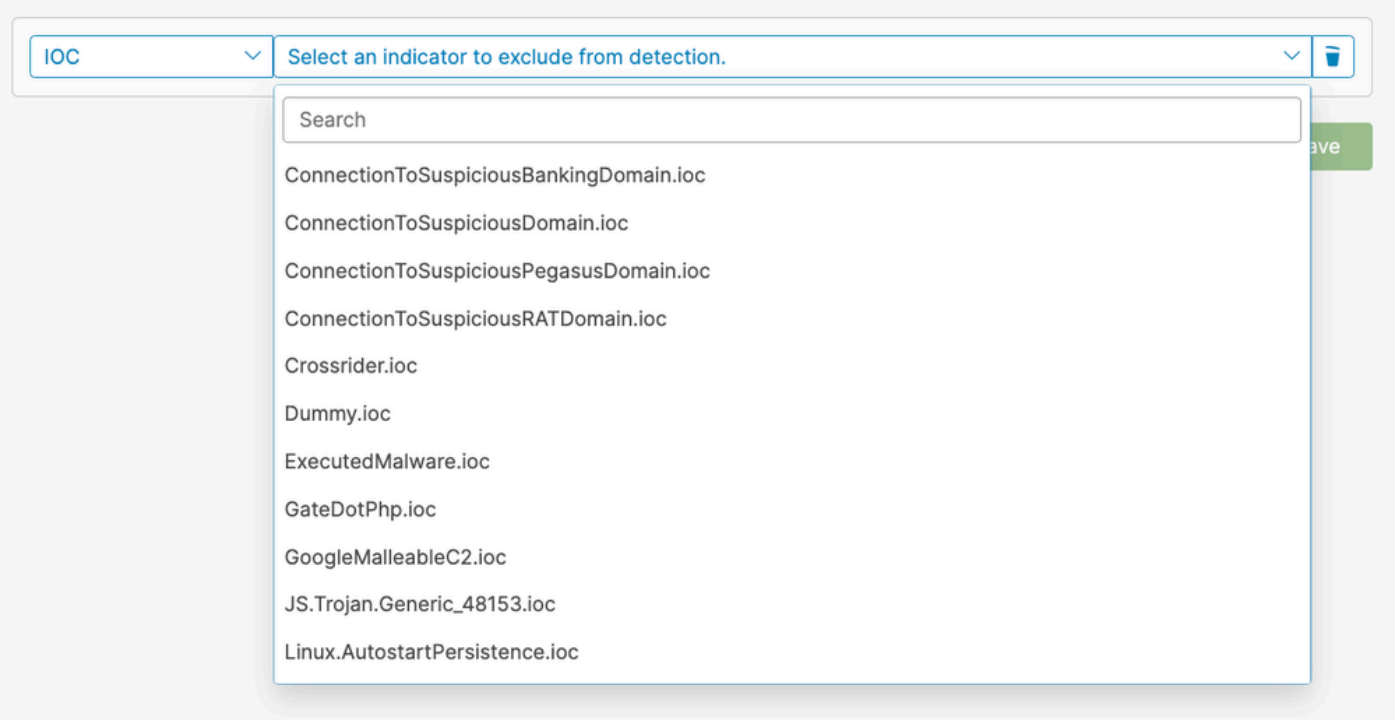


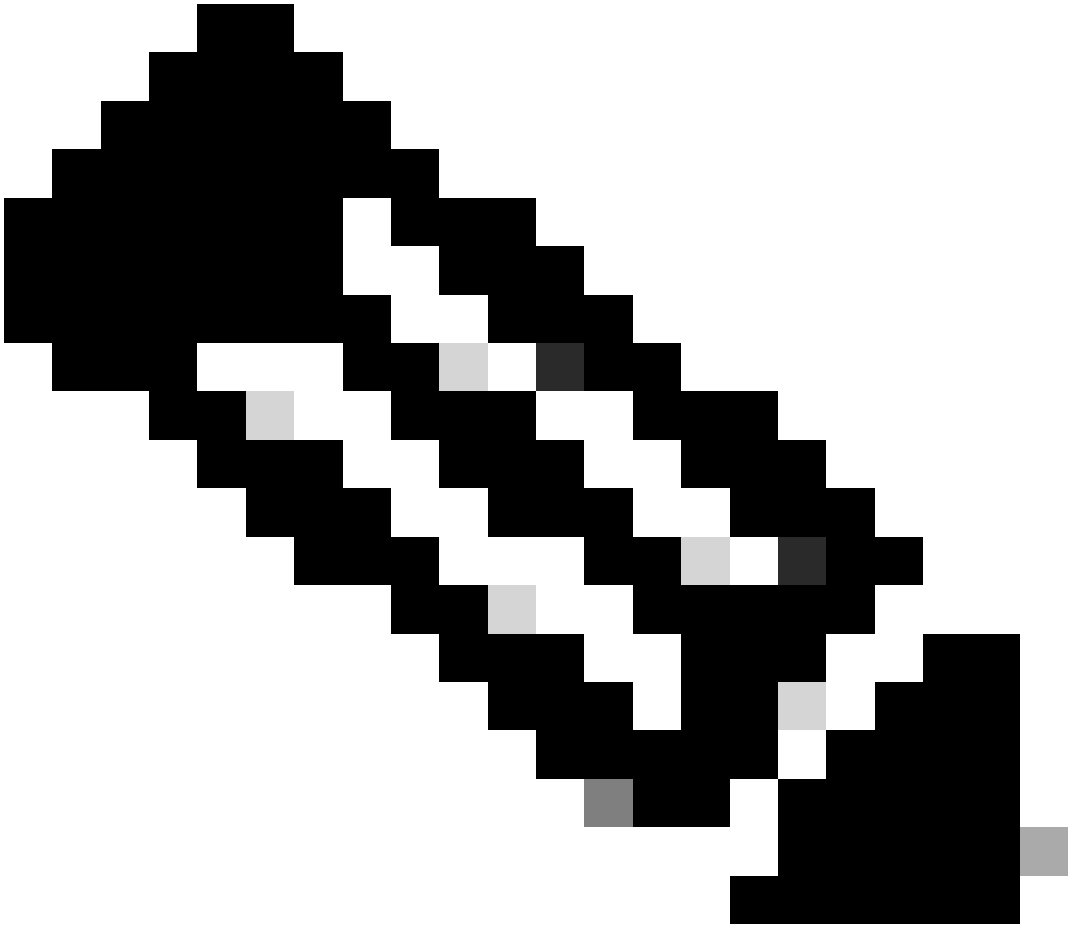
> Nota: sólo las aplicaciones se pueden excluir mediante exclusiones ejecutables mediante Secure Endpoint Console. Las exclusiones relacionadas con archivos DLL requieren la apertura de un caso de soporte para crear una exclusión.

Encontrar las exclusiones correctas para la prevención de vulnerabilidades es un proceso mucho más intensivo que cualquier otro tipo de exclusión y requiere numerosas pruebas para minimizar cualquier agujero de seguridad perjudicial.

Exclusiones de IOC (solo para Windows)

Las exclusiones de IOC le permiten excluir los indicadores de compromiso de la nube. Esto puede ser útil si tiene una aplicación personalizada o interna que puede no estar firmada y hace que ciertos IOC se activen con frecuencia. Secure Endpoint Console proporciona una lista de indicadores entre los que elegir para las exclusiones de IOC. Puede seleccionar los indicadores que desea excluir mediante un menú desplegable:


IOC
Select an indicator to exclude from detection.
Search
ConnectionToSuspiciousBankingDomain.ioc
ConnectionToSuspiciousDomain.ioc
ConnectionToSuspiciousPegasusDomain.ioc
ConnectionToSuspiciousRATDomain.ioc
Crossrider.ioc
Dummy.ioc
ExecutedMalware.ioc
GateDotPhp.ioc
GoogleMalleableC2.ioc
JS.Trojan.Generic_48153.ioc
Linux.AutostartPersistence.ioc



Nota: si excluye un IOC de gravedad alta o crítica, perderá visibilidad del mismo y podría poner en riesgo a su organización. Solo debe excluir estos IOC si experimenta un gran número de detecciones de falsos positivos para el mismo.

CSIDL y KNOWNFOLDERID (sólo para Windows)

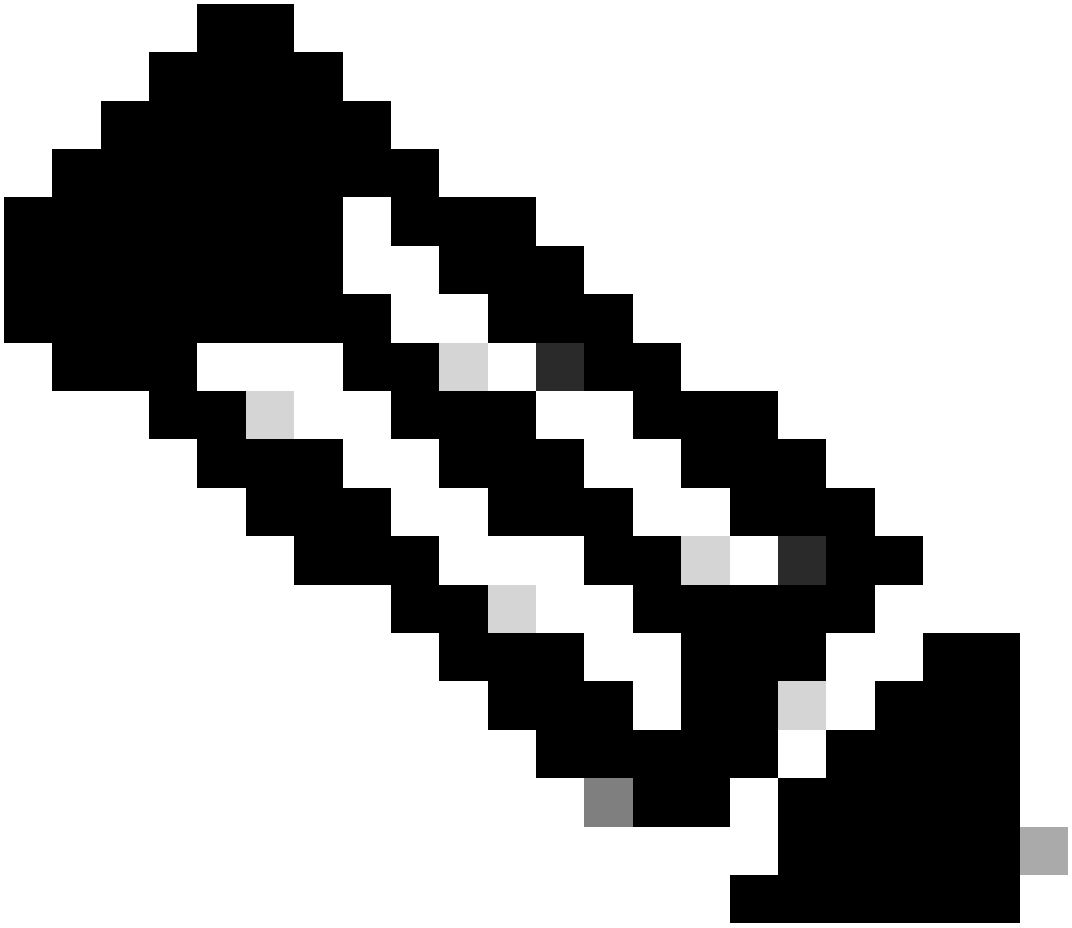
Los valores CSIDL y KNOWNFOLDERID se aceptan y se recomiendan al escribir exclusiones de procesos y rutas de acceso para Windows. Los valores CSIDL/KNOWNFOLDERID son útiles para crear exclusiones de procesos y rutas para entornos que utilizan letras de unidad alternativas.

Hay limitaciones que deben tenerse en cuenta cuando se utiliza CSIDL/KNOWNFOLDERID. Si el entorno instala programas en más de una letra de unidad, el valor CSIDL/KNOWNFOLDERID sólo hace referencia a la unidad marcada como la ubicación de instalación predeterminada o conocida.

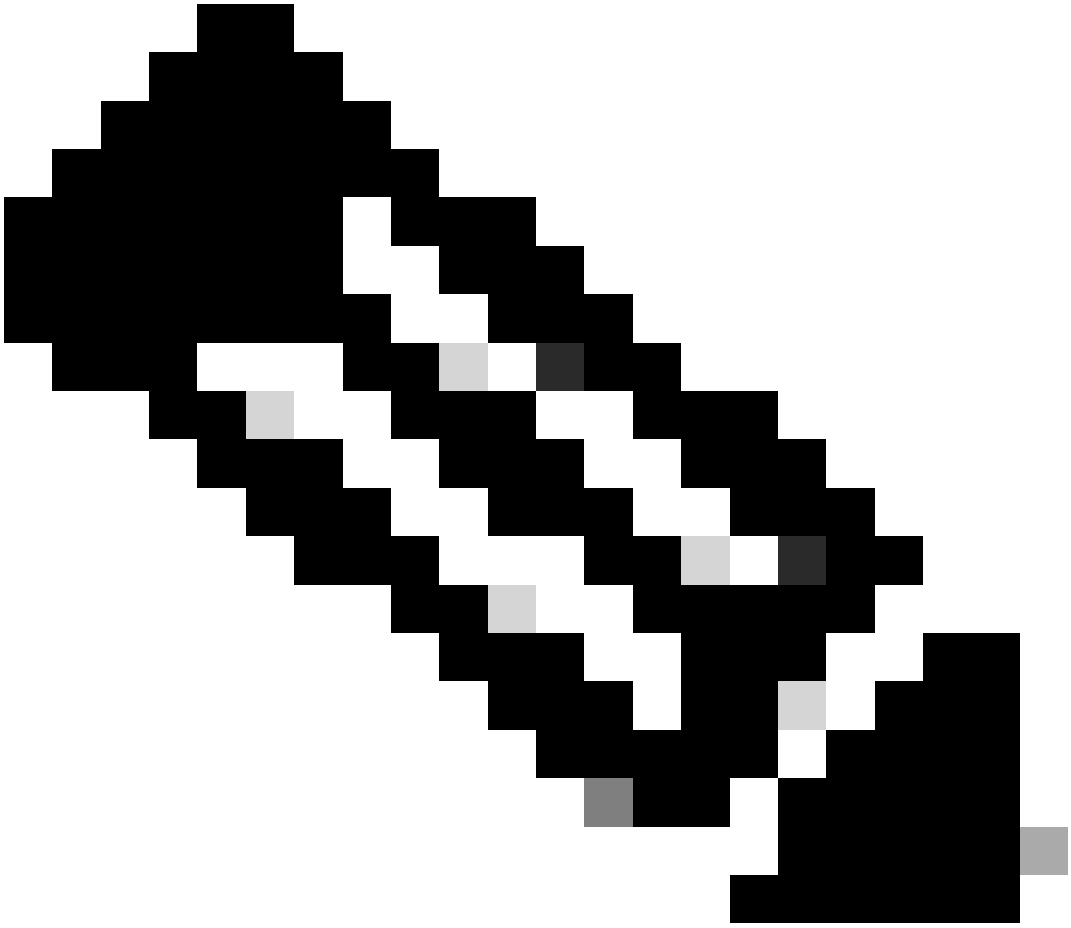
Por ejemplo, si el sistema operativo está instalado en `C:\` pero la ruta de instalación de Microsoft SQL se cambió manualmente a `D:\`, la exclusión basada en CSIDL/KNOWNFOLDERID en la lista de exclusión mantenida no se aplica a esa ruta. Esto significa que se debe ingresar una exclusión para cada ruta o exclusión de proceso que no se encuentre en la unidad `C:\` ya que el uso de CSIDL/KNOWNFOLDERID no lo mapea.

Consulte la siguiente documentación de Windows para obtener más información:

- CSIDL
- IDCARPETACONOCIMIENTO



Nota: KNOWNFOLDERID sólo se admite en el conector de Windows 8.1.7 y posteriores. Las versiones anteriores del conector de Windows utilizan valores CSIDL.



Nota: Los valores de KNOWNFOLDERID distinguen entre mayúsculas y minúsculas. Por ejemplo, debe utilizar el `valor FOLDERID_ProgramFiles` y no el `valorFolderID_programfiles` no válido.

Preparar conector para ajuste de exclusión

Para preparar el conector para el ajuste de exclusión, es necesario:

1. Configure una directiva y un grupo para que se ejecuten en modo de depuración.
2. Ejecute los equipos del nuevo grupo Depurar según las operaciones empresariales normales, deje tiempo para obtener suficientes datos del registro del conector.
3. Genere datos de diagnóstico en el conector que se utilizarán para identificar las exclusiones.

Consulte los siguientes documentos para obtener instrucciones sobre cómo habilitar el modo de depuración y recopilar datos de diagnóstico en diferentes sistemas operativos:

- Recopilación de datos de diagnóstico de Cisco Secure Endpoint Connector para Mac

- Cisco Secure Endpoint Connector para la recopilación de datos de diagnóstico de Linux
- Analizar el paquete de diagnóstico de AMP para CPU con un uso elevado (Windows)

Identificar exclusiones

MacOS y Linux

Los datos de diagnóstico generados en el modo de depuración proporcionan dos archivos útiles para crear exclusiones: fileops.txt y execs.txt. El archivo fileops.txt es útil para crear exclusiones de ruta/extensión de archivo/comodín y el archivo execs.txt es útil para crear exclusiones de proceso.

Creación de exclusiones de procesos

El archivo execs.txt enumera las rutas de acceso ejecutables que activaron Secure Endpoint para realizar un análisis de archivos. Cada ruta tiene un recuento asociado que indica cuántas veces se ha analizado y la lista se ordena en orden descendente. Puede utilizar esta lista para determinar los procesos con un gran volumen de eventos de ejecución y, a continuación, utilizar la ruta de acceso del proceso para crear exclusiones. Sin embargo, no se recomienda excluir programas de utilidad general (por ejemplo, /usr/bin/grep) o intérpretes (por ejemplo, /usr/bin/ruby). Si un programa de utilidad general o un intérprete está generando un gran volumen de análisis de archivos, puede investigar un poco más para intentar crear exclusiones más específicas:

1. Excluir el proceso padre: determine qué aplicación está ejecutando el proceso (por ejemplo, busque el proceso padre que está ejecutando grep) y excluya este proceso padre. Esto debe hacerse, si y solo si, el proceso padre puede convertirse de forma segura en una exclusión de proceso. Si la exclusión principal se aplica a los hijos, también se excluirán las llamadas a cualquier hijo del proceso principal.
2. Excluir el proceso para un usuario determinado: determinar qué usuario está ejecutando el proceso. Si un usuario específico está ejecutando el proceso a gran volumen, puede excluir el proceso solo para ese usuario específico (por ejemplo, si el usuario "root" llama a un gran volumen a un proceso, puede excluir el proceso, pero solo para el usuario 'root" especificado, esto permitirá a Secure Endpoint supervisar las ejecuciones de un proceso determinado por cualquier usuario que no sea "root").

Ejemplo de salida de execs.txt:

```
33 /usr/bin/bash
23 /usr/bin/gawk
21 /usr/bin/wc
21 /usr/bin/sleep
21 /usr/bin/ls
19 /usr/bin/pidof
17 /usr/bin/sed
14 /usr/bin/date
13 /usr/libexec/gdb
13 /usr/bin/iconv
```

```
11 /usr/bin/cat
10 /usr/bin/systemctl
 9 /usr/bin/pgrep
 9 /usr/bin/kmod
 7 /usr/bin/rm
 6 /usr/lib/systemd/systemd-cgroups-agent
 6 /usr/bin/rpm
 4 /usr/bin/tr
 4 /usr/bin/sort
 4 /usr/bin/find
```

Creación de exclusiones de ruta, extensión de archivo y comodín

El archivo fileops.txt enumera las rutas de acceso en las que el archivo crea, modifica y cambia el nombre de las actividades activadas por Secure Endpoint para realizar análisis de archivos. Cada ruta tiene un recuento asociado que indica cuántas veces se ha analizado y la lista se ordena en orden descendente. Una forma de empezar con las exclusiones de rutas de acceso es encontrar las rutas de acceso de archivos y carpetas analizadas con mayor frecuencia en fileops.txt y, a continuación, considerar la posibilidad de crear reglas para dichas rutas de acceso. Si bien un recuento alto no significa necesariamente que se deba excluir la ruta (por ejemplo, un directorio que almacena correos electrónicos se puede analizar a menudo pero no se debe excluir), la lista proporciona un punto de partida para identificar a los candidatos a la exclusión.

Ejemplo de salida de fileops.txt:

```
31 /Users/eugene/Library/Cookies/Cookies.binarycookies
24 /Users/eugene/.zhistory
9 /Users/eugene/.vim/.temp/viminfo
9 /Library/Application Support/Apple/ParentalControls/Users/eugene/2018/05/10-usage.data
5 /Users/eugene/Library/Cookies/HSTS.plist
5 /Users/eugene/.vim/.temp/viminfo.tmp
4 /Users/eugene/Library/Metadata/CoreSpotlight/index.spotlightV3/tmp.spotlight.state
3 /Users/eugene/Library/WebKit/com.apple.Safari/WebsiteData/ResourceLoadStatistics/full_browsing_sessio
3 /Library/Logs/Cisco/supporttool.log
2 /private/var/db/locationd/clients.plist
2 /Users/eugene/Desktop/.DS_Store
2 /Users/eugene/.dropbox/instance1/config.dbx
2 /Users/eugene/.DS_Store
2 /Library/Catacomb/DD94912/biolockout.cat
2 /.fseventsd/000000000029d66b
1 /private/var/db/locationd/.dat.nosync0063.arg4tq
```

Una buena regla general es que cualquier cosa con una extensión de archivo de registro o diario debe considerarse un candidato de exclusión adecuado.

Motor de protección del comportamiento

El motor de protección del comportamiento se introdujo en la versión 1.22.0 del conector Linux y en la versión 1.24.0 del conector macOS; a partir de estas versiones, el conector puede detectar

una actividad del sistema abrumadoramente alta y luego provocar la falla 18.

Las exclusiones de procesos se aplican a todos los motores y análisis de archivos. Aplique exclusiones de procesos a procesos benignos muy activos para remediar este fallo. Generado por los datos de diagnóstico del modo de depuración, el archivo top.txt se puede utilizar para determinar los procesos más activos del sistema. Consulte la guía Secure Endpoint Mac/Linux Connector Fault 18 para ver los pasos de remediación detallados.

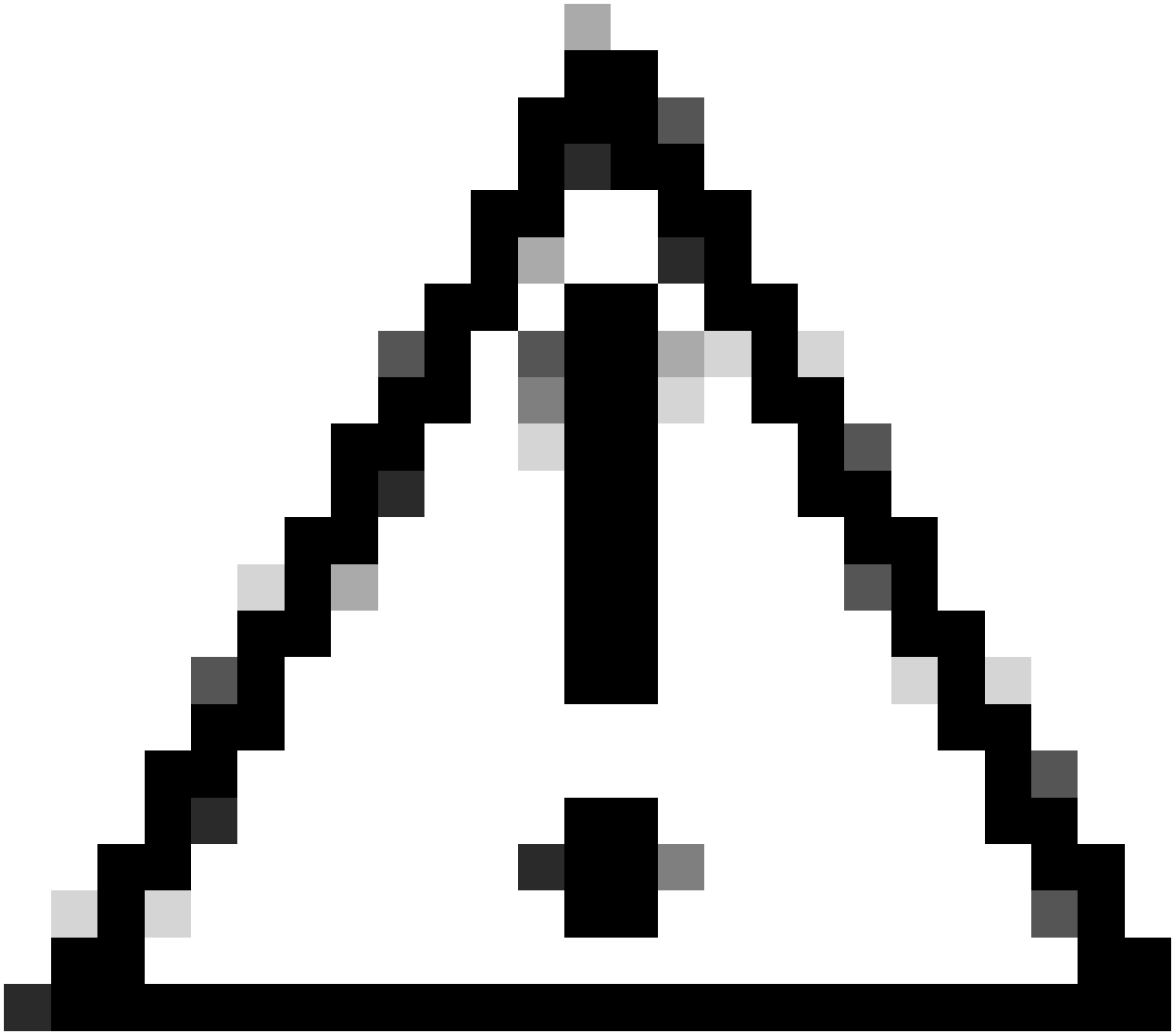
Además, las exclusiones de procesos pueden silenciar las detecciones de protección del comportamiento de falsos positivos procedentes de software benigno. Para las detecciones de falsos positivos en Secure Endpoint Console, se puede excluir el proceso para mejorar la generación de informes.

Windows:

El sistema operativo Windows es más complicado, hay más opciones de exclusión disponibles debido a los procesos primarios y secundarios. Esto indica que se requiere una revisión más profunda para identificar los archivos a los que se ha accedido, pero también los programas que los han generado.

Consulte esta Herramienta de ajuste de Windows en la página de GitHub de Seguridad de Cisco para obtener más detalles sobre cómo analizar y optimizar el rendimiento de Windows con un terminal seguro.

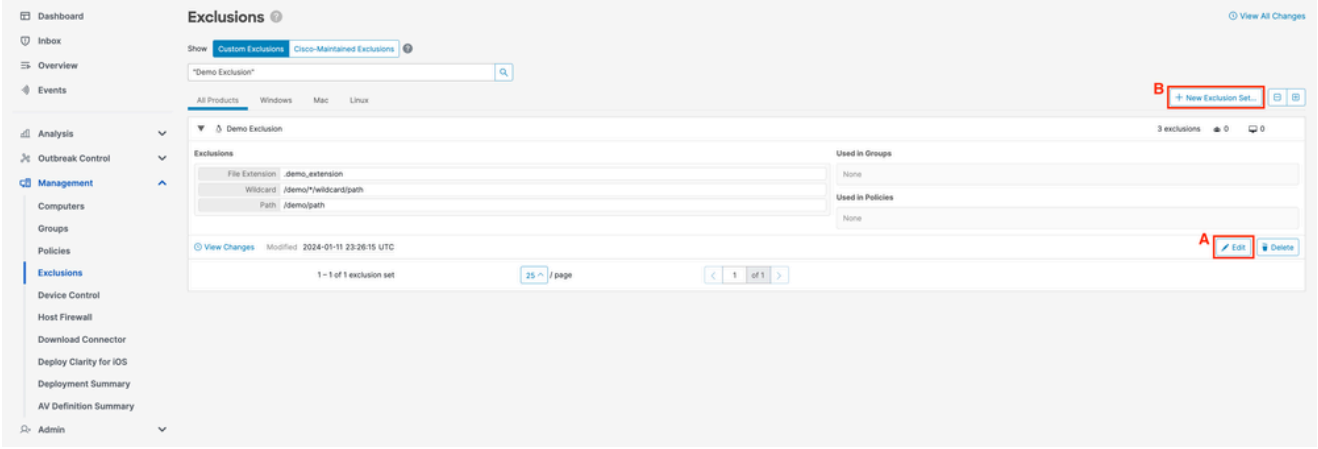
Creación de reglas de exclusión en Secure Endpoint Console



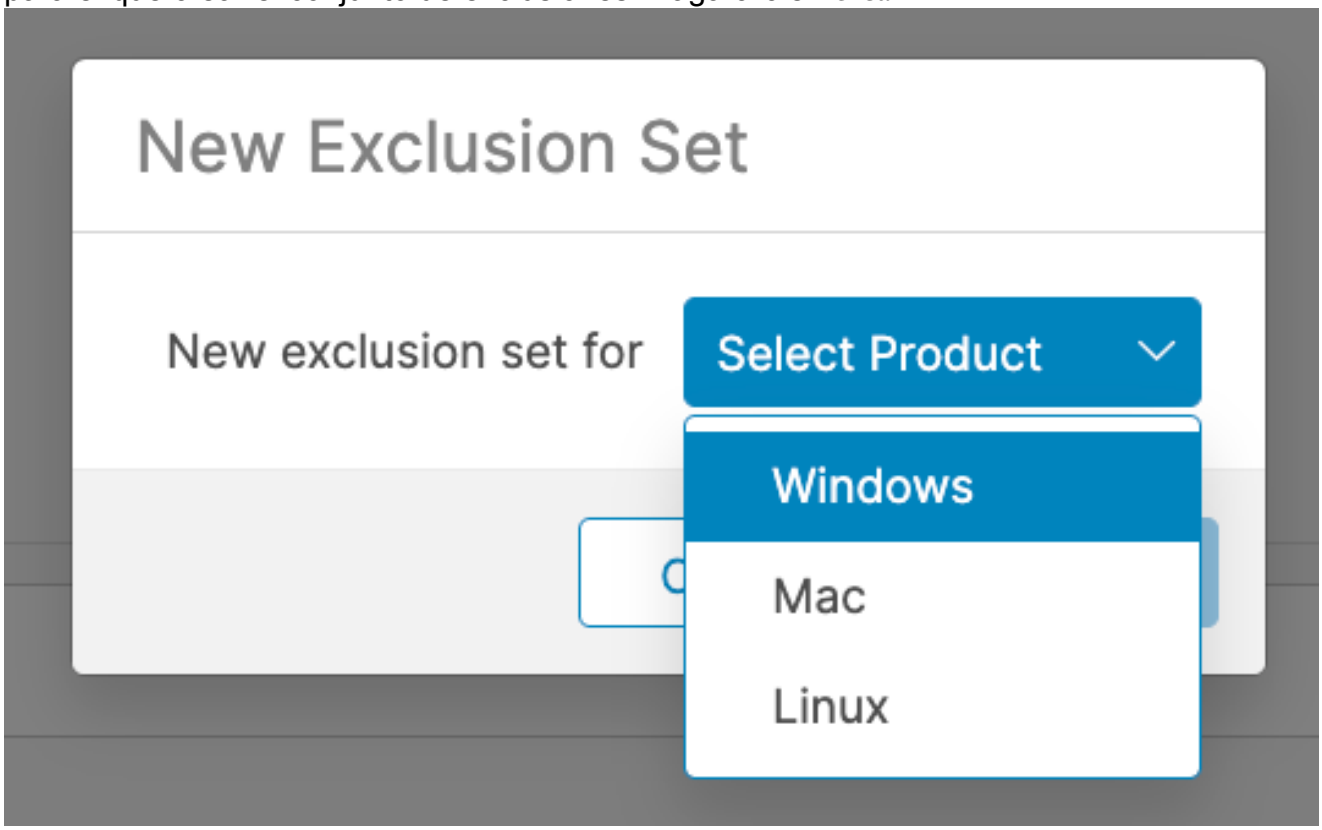
Precaución: entienda siempre los archivos y los procesos antes de escribir una exclusión para evitar vulnerabilidades de seguridad en el terminal.

Siga estos pasos para crear una nueva regla de exclusión mediante Secure Endpoint Console:

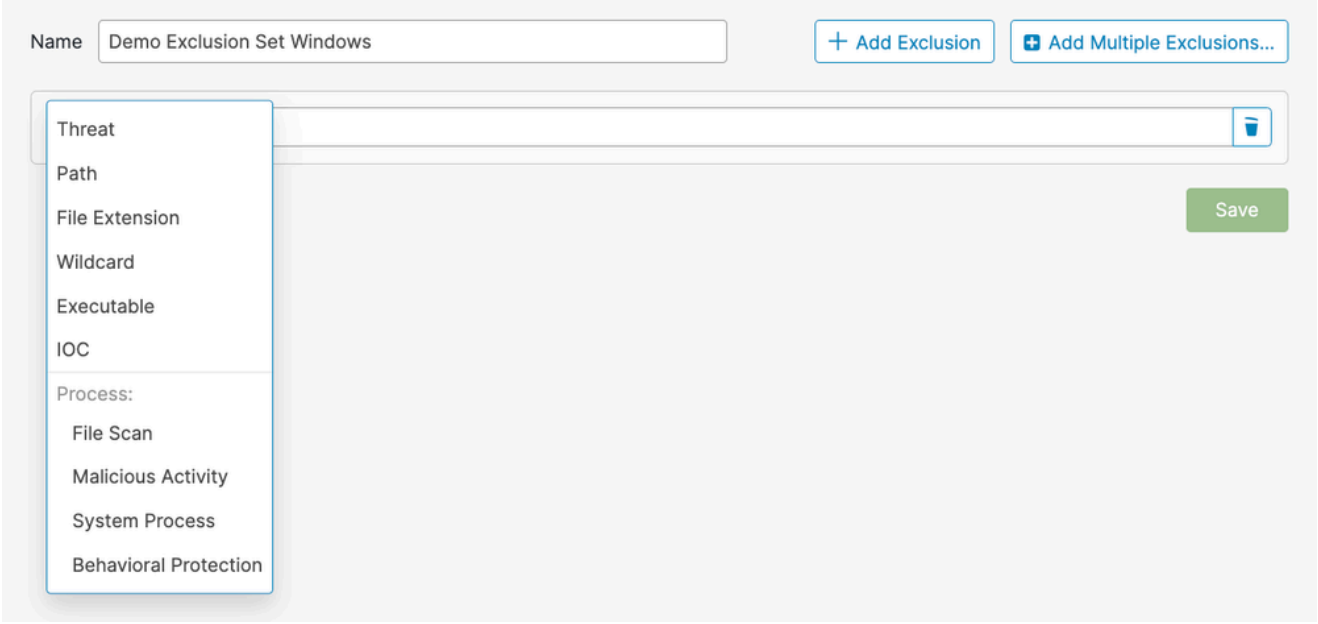
1. En Secure Endpoint Console, acceda a la página Políticas seleccionando `Management` -> `Exclusions`. A) busque el conjunto de exclusiones que desee modificar y haga clic en `Editar`, o B) haga clic en `+ Nuevo conjunto de exclusiones...`.



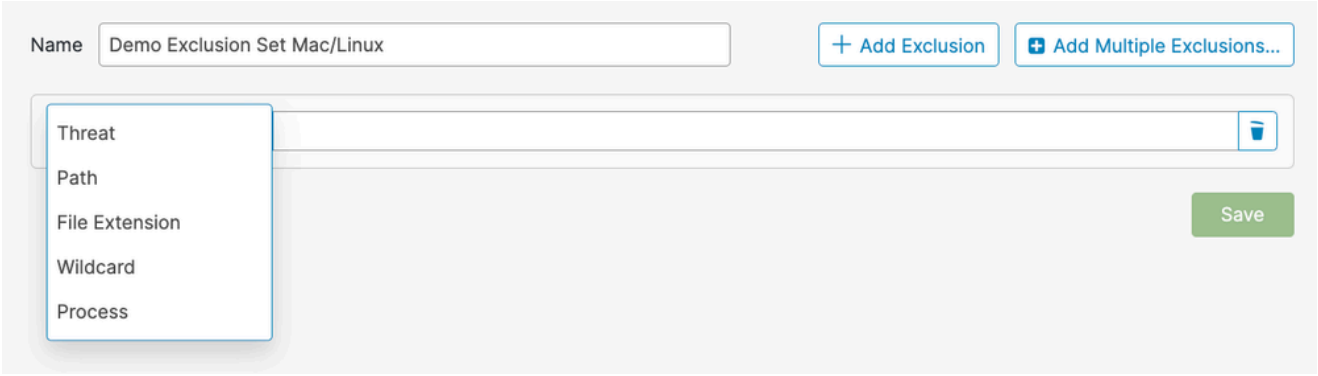
2. En la ventana emergente `Nuevo conjunto de exclusiones`, seleccione un sistema operativo para el que crear el conjunto de exclusiones. Haga clic en `Crear`.



3. Se le redirigirá a la página `Nuevo conjunto de exclusiones`. Haga clic en `+ Add Exclusion` y seleccione el tipo de exclusión en el menú desplegable `Select Type`.
   Windows:



Mac/Linux:



4. Rellene los campos obligatorios para el tipo de exclusión seleccionado.
5. Repita los pasos 2 y 3 para agregar más reglas o haga clic en `Guardar` para guardar el conjunto de exclusiones.

Mejores medidas

Tenga cuidado al crear exclusiones, ya que reducen el nivel de protección que proporciona Cisco Secure Endpoint. Los archivos excluidos no se trocean, analizan ni están disponibles en la caché o la nube, la actividad no se supervisa y falta información en los motores backend, la trayectoria de los dispositivos y el análisis avanzado.

Las exclusiones solo se deben utilizar en casos específicos, como problemas de compatibilidad con aplicaciones específicas o problemas de rendimiento que no se pueden mejorar de otro modo.

Algunas prácticas recomendadas para crear exclusiones son las siguientes:

- Crear exclusiones únicamente para problemas probados
  - No asuma que una exclusión es necesaria a menos que se demuestre que ha sido un problema que no se puede solucionar de otra manera.
  - Los problemas de rendimiento, los falsos positivos o los problemas de compatibilidad de las aplicaciones deben investigarse a fondo y mitigarse antes de aplicar una

exclusión.

- Preferir exclusiones de procesos a exclusiones de rutas, extensiones de archivos o comodines
  - Las exclusiones de procesos proporcionan una forma más directa de excluir actividades de software benignas que utilizar una combinación de exclusiones de ruta, extensión de archivo y comodín para obtener el mismo resultado.
  - Se recomienda reemplazar, cuando sea posible, las exclusiones Path, File Extension y Wildcard dirigidas a los ejecutables del programa por las exclusiones Process correspondientes.
- Evitar las exclusiones generales
  - No excluya grandes partes del terminal, como la unidad C completa.
  - Utilice la ruta de acceso completa al archivo en lugar de sólo el nombre de archivo.
  - Utilice la trayectoria del dispositivo, los datos de diagnóstico de terminales seguros y la herramienta de ajuste de Windows para investigar y determinar exclusiones específicas.
- Evitar el uso excesivo de exclusiones de comodines
  - Tenga cuidado al crear exclusiones con comodines. Utilice exclusiones más específicas cuando sea posible.
  - Utilice la cantidad mínima de comodines en una exclusión; sólo las carpetas que son realmente variables deben utilizar un comodín.
- Evite excluir programas de utilidad general e intérpretes
  - No se recomienda excluir los programas de utilidad general o los intérpretes.
  - Si necesita excluir un programa de utilidad general o intérpretes, proporcione un usuario de proceso (solo macOS/Linux).
  - Por ejemplo, evite escribir exclusiones que incluyan python, `java`, `ruby`, `bash`, sh, etc.
- Evitar exclusiones duplicadas
  - Antes de crear una exclusión, compruebe si ya existe en las exclusiones personalizadas o en las exclusiones mantenidas por Cisco.
  - La eliminación de exclusiones duplicadas mejora el rendimiento y reduce la gestión operativa de las exclusiones.
  - Asegúrese de que la ruta de acceso especificada en una exclusión de proceso no esté cubierta por una exclusión de ruta de acceso, extensión de archivo o comodín.
- Evite excluir procesos conocidos por su uso habitual en ataques de malware
  - Consulte Exclusiones no recomendadas para obtener más detalles.
- Eliminar exclusiones obsoletas
  - Revise y audite regularmente su lista de exclusiones y mantenga un registro de por qué se agregaron ciertas exclusiones.
- Eliminar exclusiones al comprometer
  - Las exclusiones deben eliminarse si un conector está comprometido para recuperar una seguridad y visibilidad óptimas.
  - Las acciones automatizadas se pueden utilizar para aplicar políticas más seguras a los conectores después de la infección. Si un conector se ve comprometido, debe trasladarse a un grupo que contenga una política sin exclusiones para garantizar que se aplica el nivel más alto de protección.
  - Consulte Identificación de condiciones para desencadenar acciones automatizadas en un terminal seguro para obtener más detalles sobre cómo configurar proactivamente la

acción automatizada "Mover equipo a un grupo si hay algún riesgo".

- Aumentar la protección de los elementos excluidos
  - Cuando las exclusiones sean absolutamente necesarias, considere qué tácticas de mitigación se pueden tomar, como habilitar la protección contra escritura para agregar algunas capas de protección para los elementos excluidos.
- Crear exclusiones de forma inteligente
  - Optimice las reglas seleccionando el proceso principal de nivel superior que identifica de forma única la aplicación que se va a excluir y utilice la opción `Aplicar al proceso secundario` para minimizar el número de reglas.
- No excluir nunca el proceso de inicio
  - El proceso de inicio (`iniciado` en macOS, `init` o `systemd` en Linux) es responsable de iniciar todos los demás procesos en el sistema y está en la parte superior de la jerarquía de procesos.
  - Si se excluye el proceso de inicio y todos sus procesos secundarios, se deshabilitaría de forma efectiva la supervisión de terminales seguros.
- Especifique el usuario del proceso cuando sea posible (solo macOS/Linux)
  - Si el campo de usuario se deja en blanco, la exclusión se aplica a cualquier proceso que ejecute el programa especificado.
  - Si bien una exclusión que se aplica a cualquier usuario es más flexible, este amplio ámbito podría excluir involuntariamente la actividad que se debe supervisar.
  - La especificación del usuario es especialmente importante para las reglas que se aplican a programas compartidos como motores de tiempo de ejecución (por ejemplo, `java`) e intérpretes de secuencias de comandos (por ejemplo, `bash`, `python`).
  - Al especificar el usuario, se limita el alcance y se indica a Secure Endpoint que ignore instancias específicas mientras se supervisan otras instancias.

Exclusiones no recomendadas

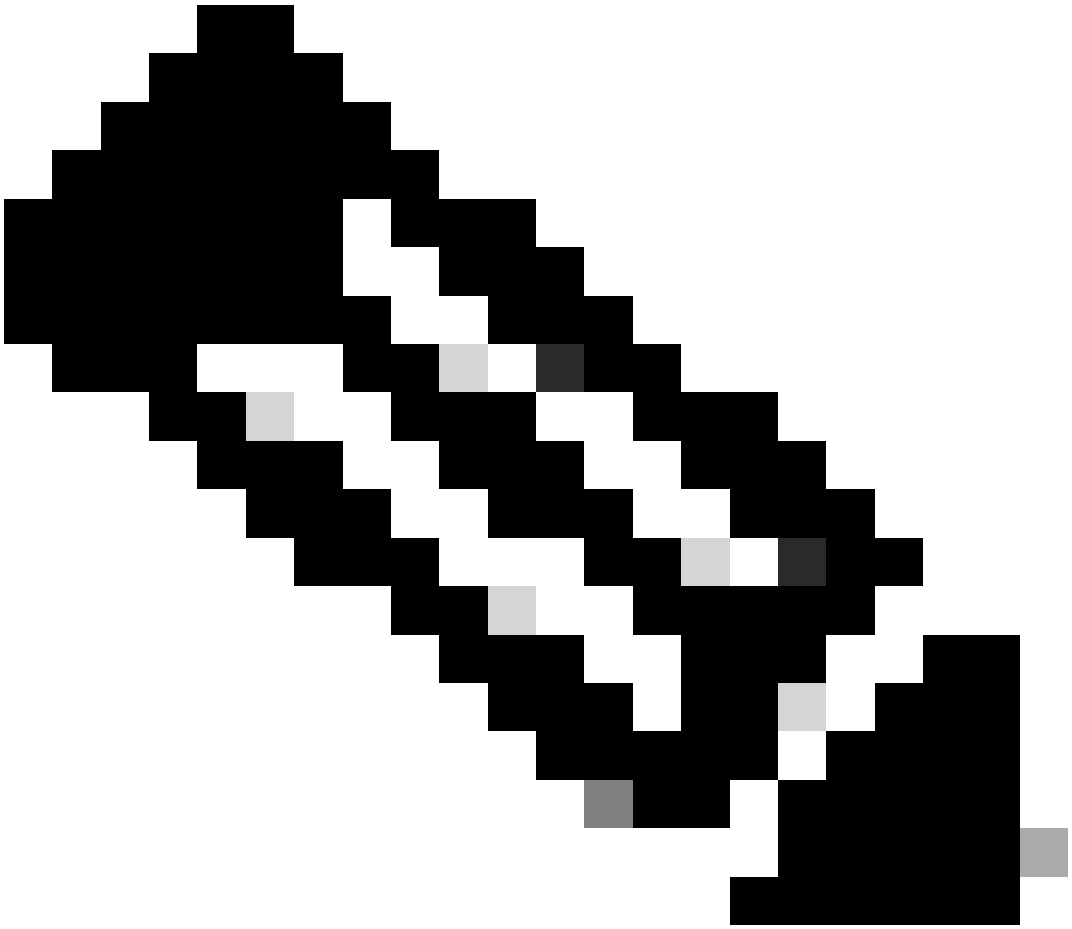
Aunque es imposible conocer todos los vectores de ataque posibles que puede utilizar un adversario, hay algunos vectores de ataque principales que se deben supervisar. Para mantener un buen estado de seguridad y visibilidad, no se recomiendan las siguientes exclusiones:

AcroRd32.exe
addinprocess.exe
addinprocess32.exe
addinutil.exe
bash.exe
bginfo.exe
bitsadmin.exe
cdb.exe
csi.exe
dbghost.exe
dbgsvc.exe
dnx.exe
dotnet.exe

excel.exe
fsi.exe
fsiAnyCpu.exe
iexplore.exe
java.exe
kd.exe
lxssmanager.dll
msbuild.exe
mshta.exe
ntkd.exe
ntsd.exe
outlook.exe
psexec.exe
powerpnt.exe
powershell.exe
rcsi.exe
svchost.exe
schtasks.exe
system.management.automation.dll
windbg.exe
winword.exe
wmic.exe
wuauclt.exe
0,7z
.bat
.bin
.cab
.cmd
.com
.cpl
.dll
.exe
.fla
.gif
.gz
.hta
.inf
.java
.jar
.job
.jpeg
.jpg

.js
.ko
.ko.gz
.msi
.ocx
.png
.ps1
.py
.rar
.reg
.scr
.sys
.tar
.tmp
.url
.vbe
.vbs
.wsf
.zip
golpear
java
pitón
Python3
sh
zsh
/
/bin
/sbin
/usr/lib
C:
C:\
C:*
D:\
D:*
C:\Program Files\Java
C:\Temp\
C:\Temp*
C:\Users\
C:\Users*
C:\Windows\Prefetch
C:\Windows\Prefetch\

C:\Windows\Prefetch*
C:\Windows\System32\Spool
C:\Windows\System32\CatRoot2
C:\Windows\Temp
C:\Windows\Temp\
C:\Windows\Temp*
C:\Program Archivos\<nombre de la empresa>\
C:\Program Archivos (x86)\<nombre de la empresa>\
C:\Users\<UserProfileName>\AppData\Local\Temp\
C:\Users\<UserProfileName>\AppData\LocalLow\Temp\



Nota: esta no es una lista exhaustiva de exclusiones que se deben evitar, pero proporciona información sobre los vectores de ataque principales. Es fundamental mantener la visibilidad de estas rutas, extensiones de archivos y procesos.

Información Relacionada

- Soporte Técnico y Documentación - Cisco Systems
- Terminal seguro de Cisco - Notas técnicas
- Cisco Secure Endpoint - Guía del usuario
- Solución de problemas de prevención de vulnerabilidades en terminales seguros
- Identificar las condiciones para desencadenar acciones automatizadas en un terminal seguro

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).