配置和辨識安全終端排除

目錄

簡介

本文檔介紹什麼是排除、如何辨識排除，以及在思科安全終端上建立排除的最佳實踐。

免責宣告

本文檔中的資訊基於Windows、Linux和macOS作業系統。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

概觀

閱讀本檔案後，您應該瞭解：

- 什麼是exclusion？Cisco Secure Endpoint可用的不同排除型別。
- 如何準備聯結器以進行排除調整。
- 如何辨識潛在的強大排除。
- 如何在Cisco Secure Endpoint Console中建立新排除項。
- 建立排除項的最佳實踐是什麼？

何謂排除？

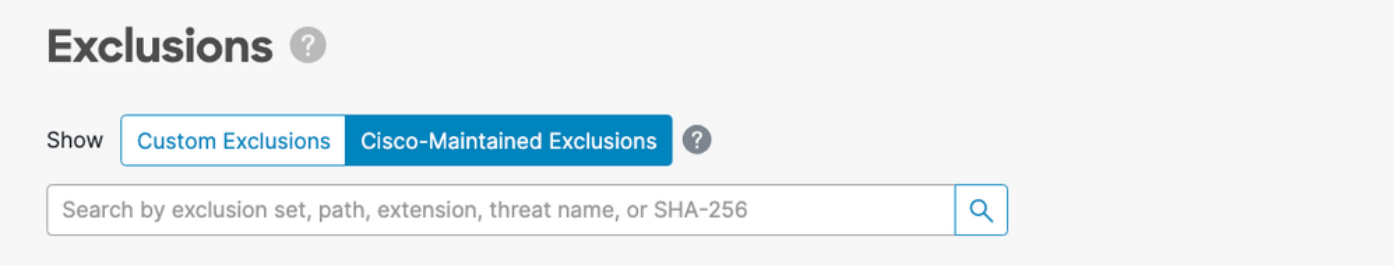
排除集是目錄、副檔名、檔案路徑、進程、威脅名稱、應用程式或不希望聯結器掃描或定罪的危害表現清單。當啟用終端保護（如安全終端）時，需要精心編制排除，以確保電腦上的效能和安全性達到平衡。本文描述Secure Endpoint Cloud、TETRA、SPP和MAP的排除。

每個環境都是獨一無二的，控制它的實體也各不相同，從嚴格的政策到開放的政策。因此，排除必須針對每種情況專門制定。

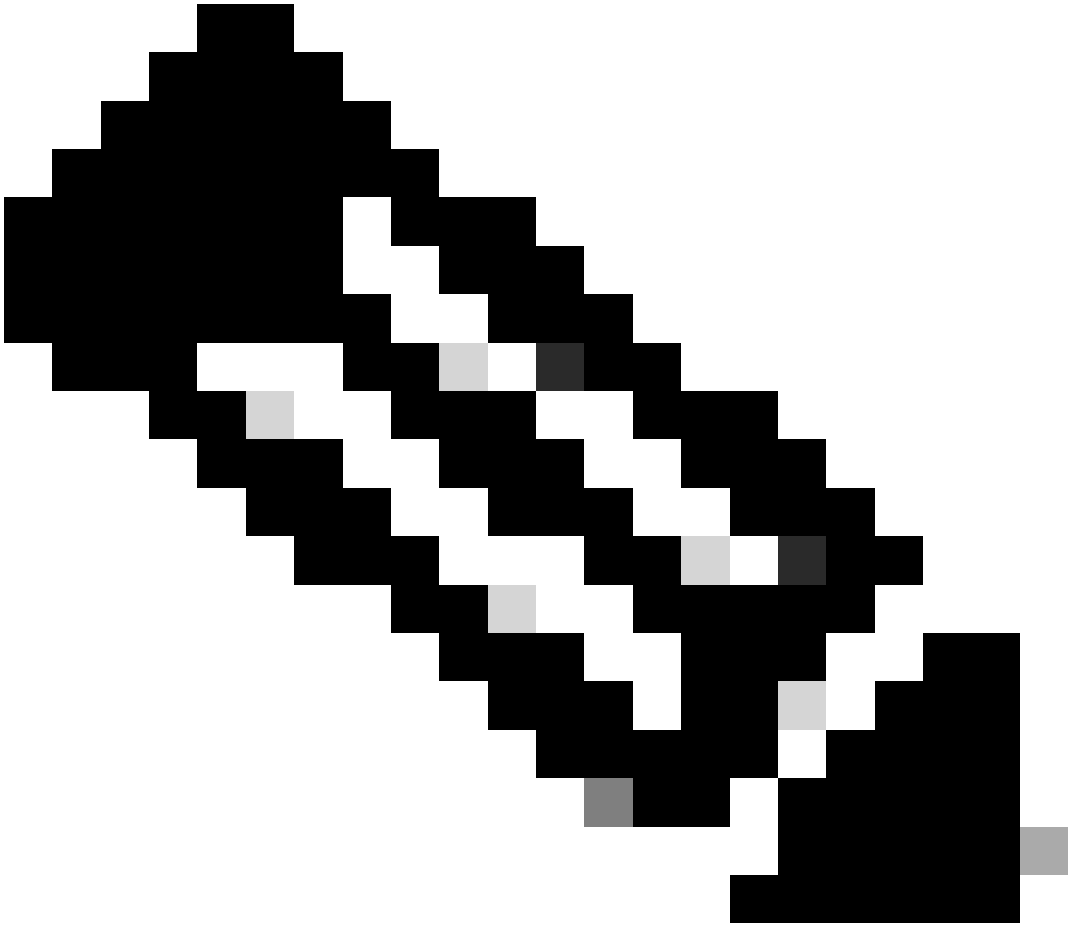
排除項可以採用兩種方式分類：思科維護的排除項和自定義排除項。

思科維護的排除

思科維護的排除項是根據研究建立並對常用作業系統、程式和其他保安軟體進行嚴格測試的排除項。在排除頁面的「安全終端控制檯」中選擇思科維護的排除可顯示這些排除。



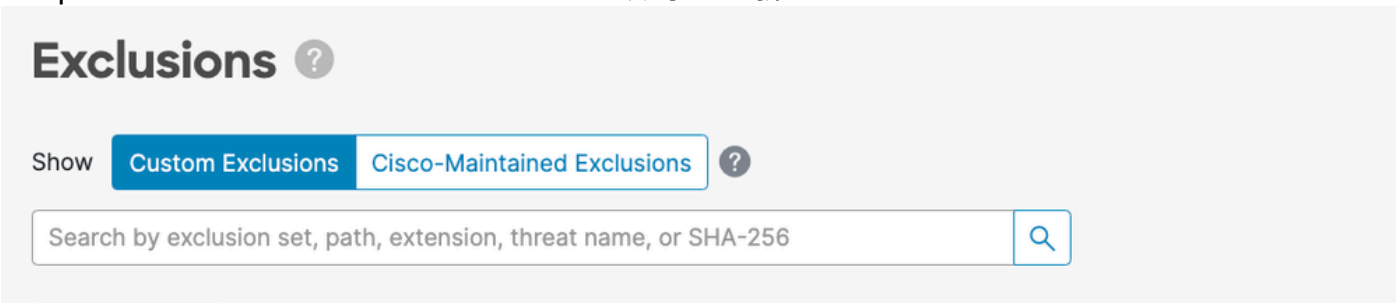
思科監控防病毒(AV)供應商發佈的推薦排除清單，並更新思科維護的排除項以包括推薦的排除項。



注意：某些AV供應商可能不會發佈其建議的排除項。在這種情況下，客戶可能需要聯絡AV供應商以請求建議排除的清單，然後提交支援案例以更新思科維護的排除項。

自定義排除

自定義排除項是使用者為終端上的自定義使用案例建立的排除項。在Exclusions頁面的Secure Endpoint Console中選擇Custom Exclusions可顯示這些排除。



排除的型別

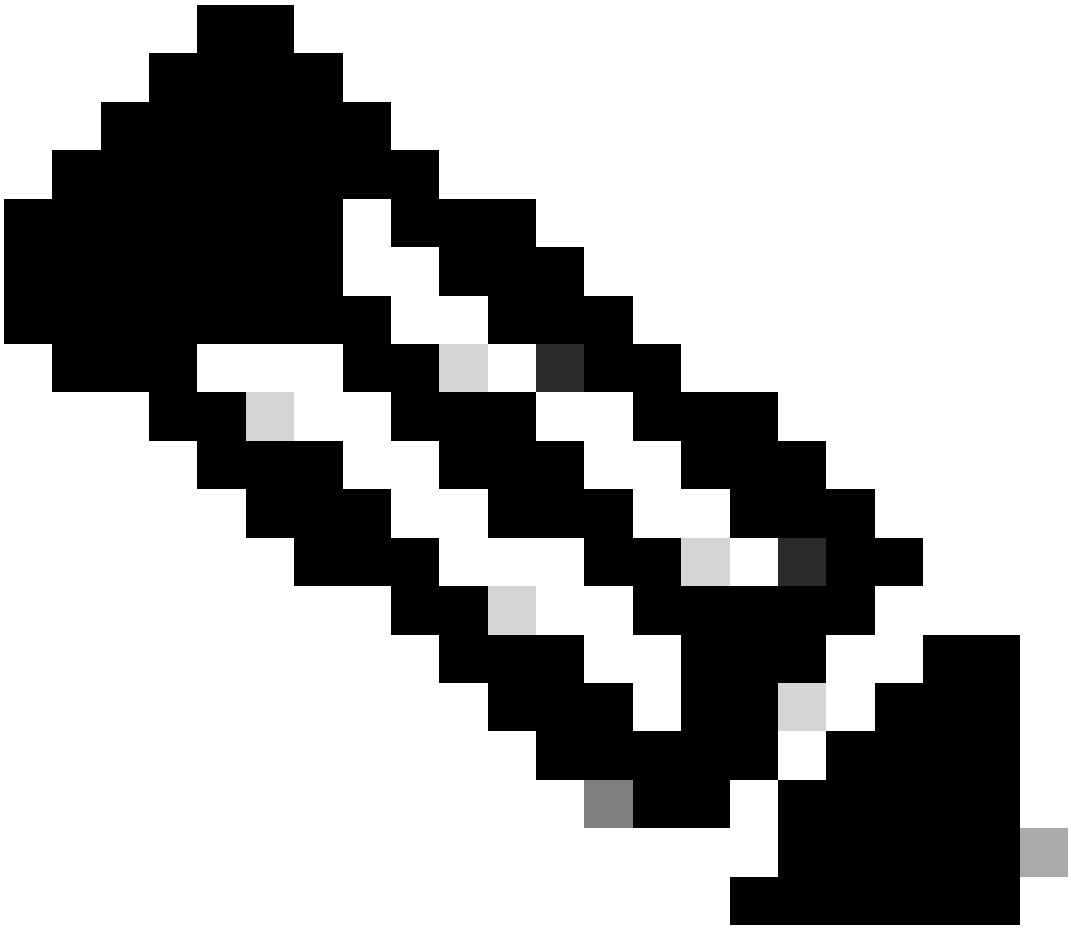
處理序排除

程式排除允許系統管理員從支援的引擎排除程式。下表列出了每個平台上支援進程排除的引擎：

作業系統	引擎			
	檔案掃描	系統程式保護	惡意活動防護	行為保護
Windows	✓	✓	✓	✓
Linux	✓	✗	✗	✓
macOS	✓	✗	✗	✓

MacOS和Linux

您必須在建立「程式排除」時提供絕對路徑，也可以提供選擇性的使用者。如果您同時指定路徑和使用者，則必須同時符合這兩個條件，才能排除流程。如果未指定使用者，則進程排除將應用於所有使用者。



注意：在macOS和Linux上，進程排除項適用於所有引擎。

處理萬用字元：

安全終端Linux和macOS聯結器支援使用進程排除中的萬用字元。這允許擴大覆蓋範圍，但排除的情形更少，但如果太多未定義就很危險。您必須只使用萬用字元來涵蓋提供所需排除項所需的最少字元數。

在macOS和Linux中使用進程萬用字元：

- 萬用字元由單一星號字元(*)表示
- 萬用字元可以用來取代單一字元或完整目錄。
- 將萬用字元放在路徑的開頭會視為無效。
- 萬用字元可在兩個定義的字元（斜線或英數字元）之間使用。

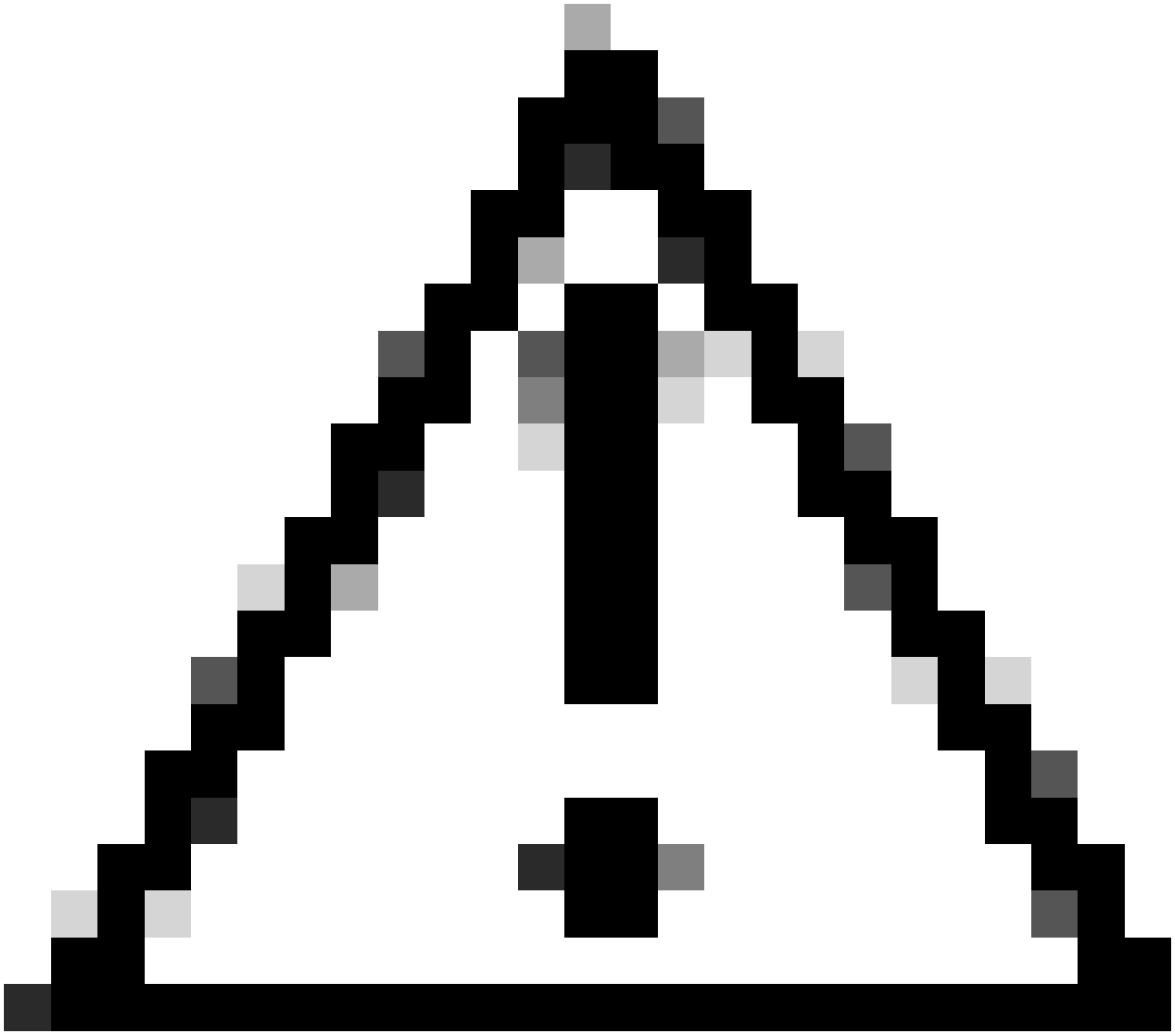
範例：

排除	預期結果
`/Library/Java/JavaVirtualMachines/*/java`	排除`JavaVirtualMachines`所有子資料夾中的`java`
`/Library/Jibber/j*bber`	排除`jabber`、`jibber`、`jobber`等進程

Windows

建立進程排除時，您可以提供進程執行檔的絕對路徑和/或SHA-256。如果同時指定路徑和SHA-256，則必須同時滿足這兩個條件，才能排除進程。

在Windows上，您也可以在路徑中使用CSIDL或KNOWNFOLDERID來建立進程排除。

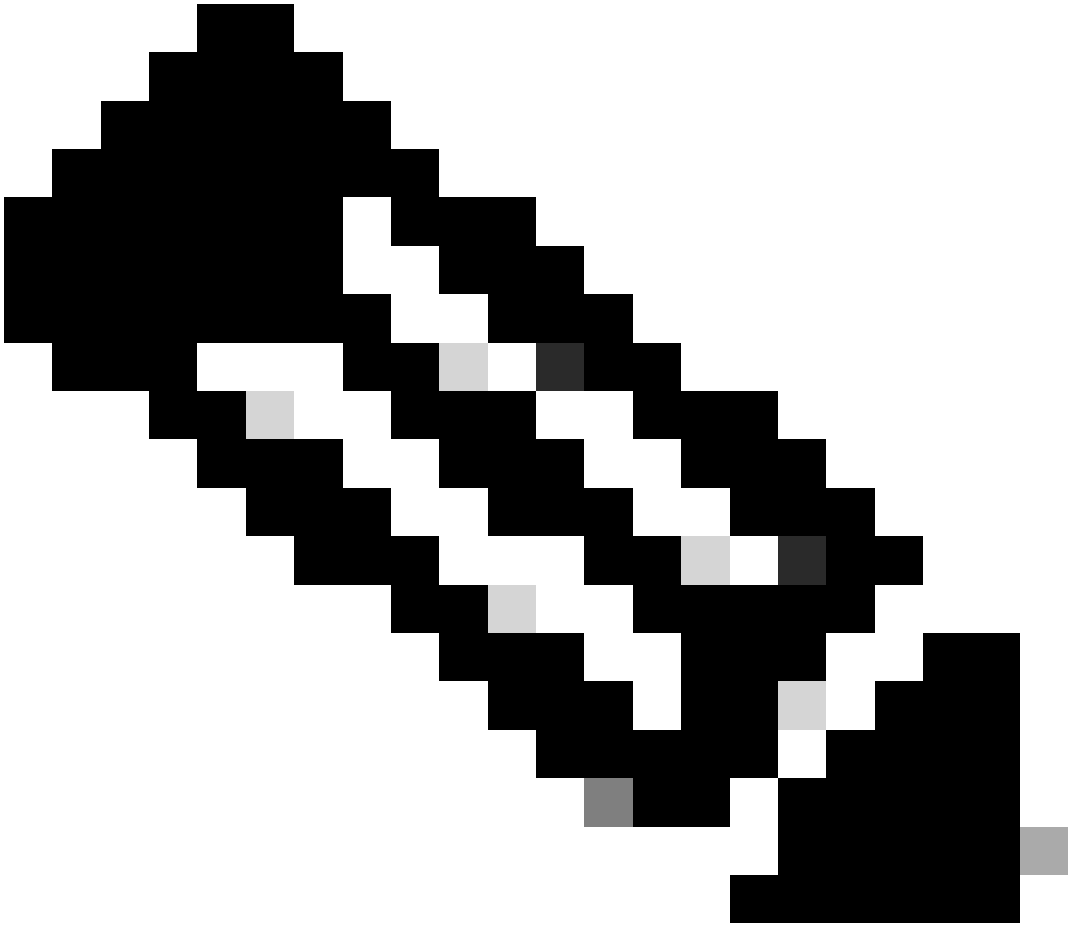


注意：預設不會排除已排除處理作業建立的子處理作業。若要在建立排除程式時排除其他程式，請選取套用至子程式。

限制：

- 如果進程的檔案大小大於策略中設定的掃描檔案大小上限，則不會計算進程的SHA-256，不會運行排除。對大於掃描檔案大小上限的檔案使用基於路徑的進程排除。
- Windows聯結器對所有進程排除型別強制實施最多500個進程排除。
  - 從policy.xml中進程排除清單的頂部開始，進程排除只遵從限制。
  - 每個Windows策略都有sfc.exe的進程排除，這取決於進程排除限制：

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



注意：在Windows上，處理序排除會套用至每個引擎。如果相同排除應用於多個引擎，則在此例中必須為每個適用的引擎複製進程排除。

處理萬用字元：

安全終端Windows聯結器支援使用進程排除中的萬用字元。這允許擴大覆蓋範圍，但排除的情形更少，但如果太多未定義就很危險。您必須只使用萬用字元來涵蓋提供所需排除項所需的最少字元數。

Windows進程萬用字元的使用：

- 萬用字元由單一星號字元()和雙星號(*)表示
- 單星號萬用字元(*)：
  - 萬用字元可以用來取代單一字元或完整目錄。
  - 將萬用字元放在路徑的開頭會視為無效。
  - 萬用字元可在兩個定義的字元（斜線或英數字元）之間使用。
  - 將萬用字元置於路徑結尾會排除該目錄中的所有程式，但不會排除子目錄中的程式。

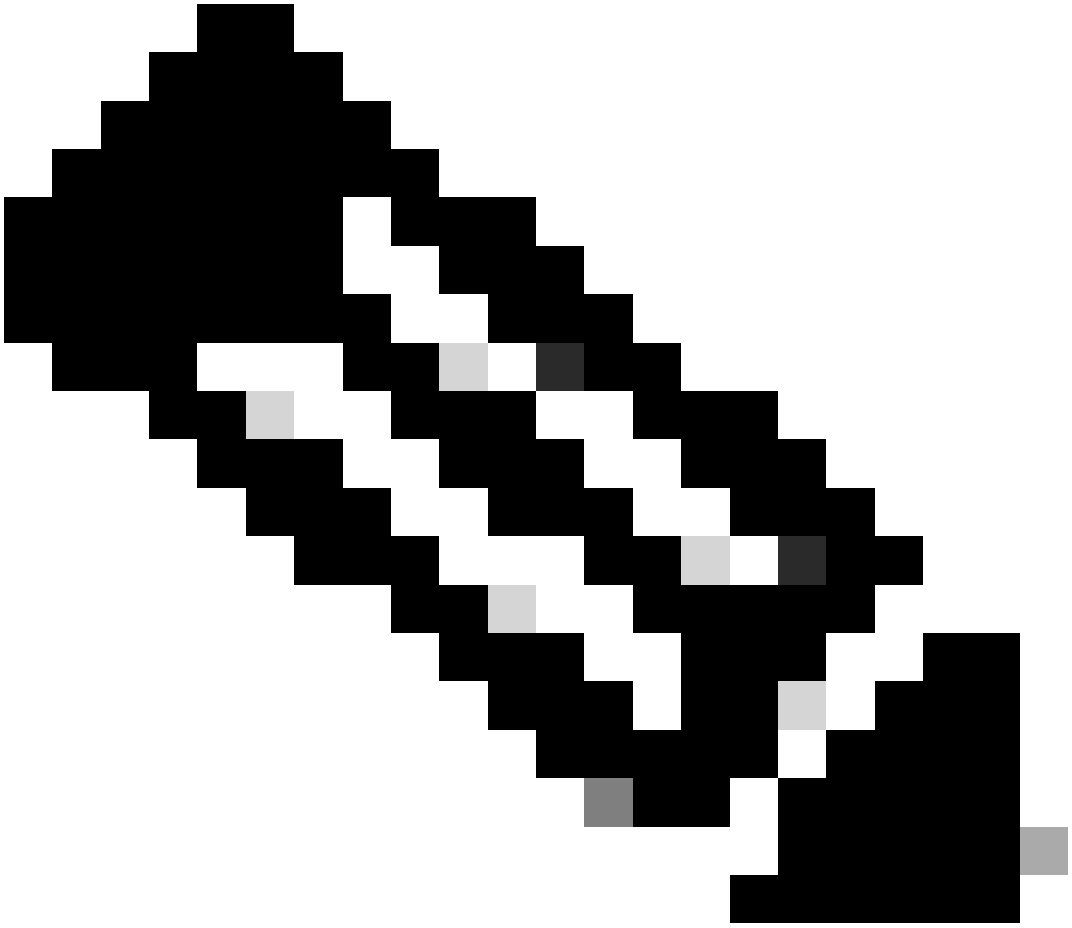
- 雙星號萬用字元(**)：
  - 只能放置在路徑的末端。
  - 將萬用字元置於路徑結尾會排除該目錄中的所有程式及子目錄中的所有程式。
  - 這允許在最小輸入的情況下使用更大的排除集，但也會為可見性留下非常大的安全漏洞。請謹慎使用此功能。

範例：

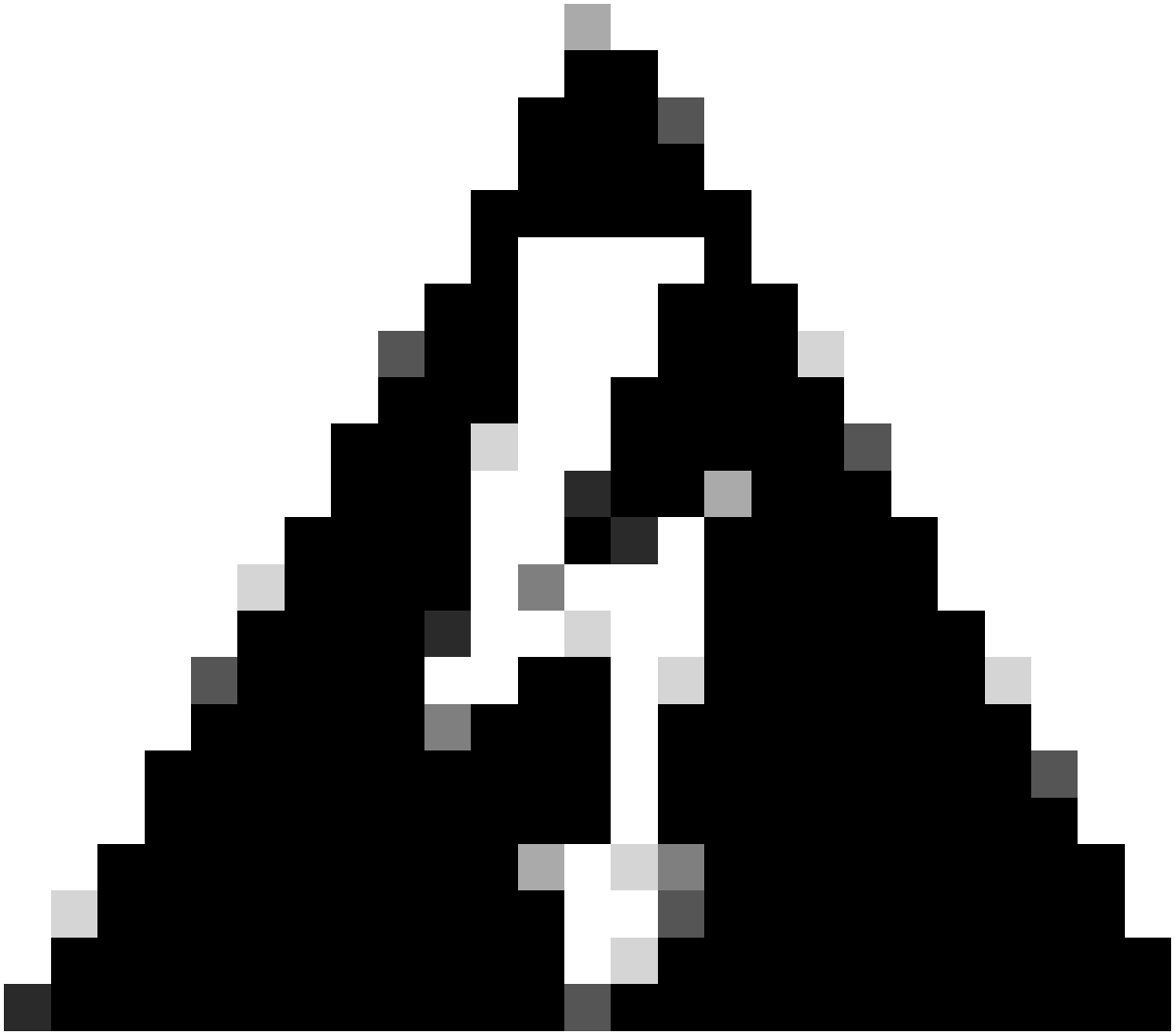
排除	預期結果
C:\Windows*\Tiworker.exe	排除在Windows子目錄中找到的所有Tiworker.exe進程
C:\Windows\P*t.exe	不包括Pot.exe、Pat.exe、P1t.exe等
C:\Windows*chairs.exe	排除Windows目錄中以jages.exe結尾的所有進程
C:*	排除C：驅動器中的所有進程，但不排除子目錄中的進程
C:**	排除C：驅動器上的每個進程

威脅排除

透過威脅排除，您可以排除特定威脅名稱來觸發事件。只有在確定事件是誤報檢測的結果時，才應使用威脅排除。在這種情況下，請使用事件的確切威脅名稱作為您的威脅排除。請注意，如果您使用此類排除，則即使對威脅名稱進行了真正肯定的檢測，也不會被檢測、隔離或生成事件。



注意：威脅排除項不區分大小寫。示例：`W32.Zombies.NotAVirus` 和w32.zombies.notavirus都匹配相同的威脅名稱。



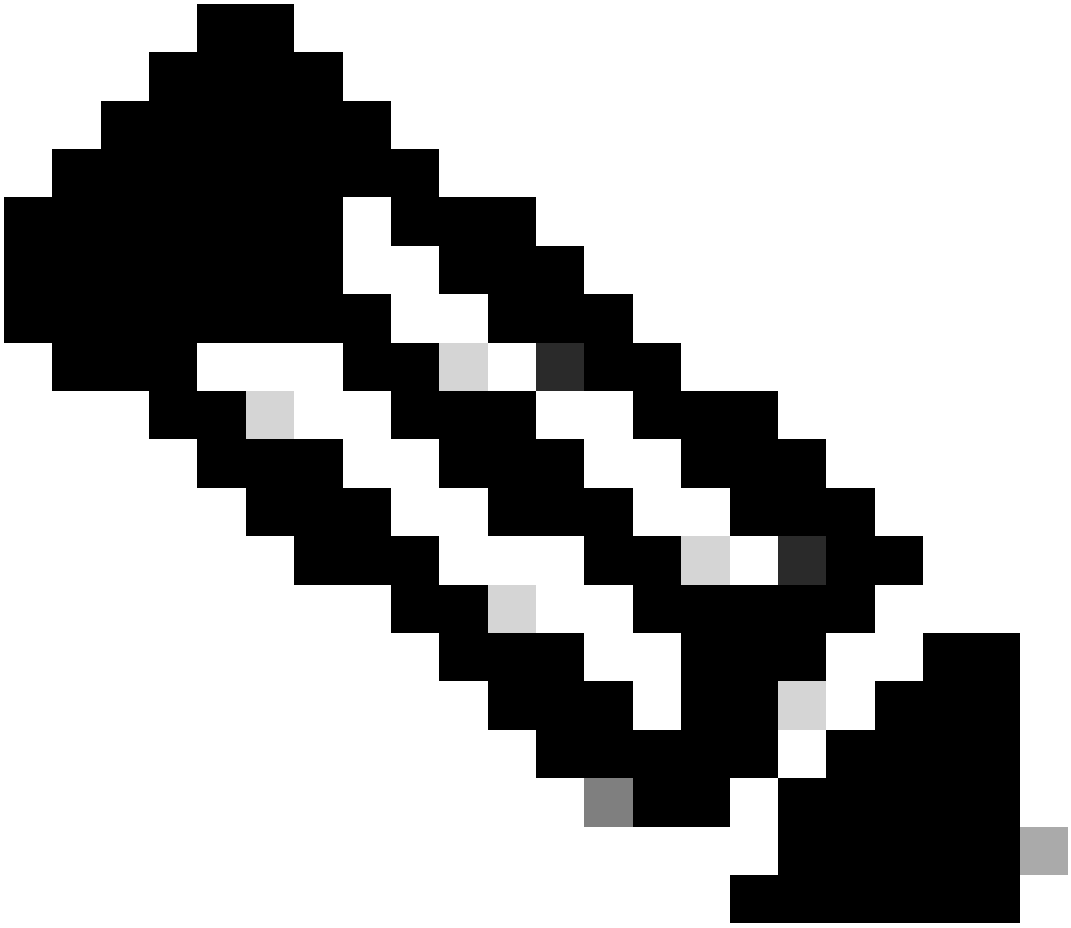
警告：除非經過徹底調查確認威脅名稱為誤報，否則不要排除威脅。排除的威脅不再填充events（事件）頁籤進行檢視和稽核。

路徑排除

路徑排除是最常用的方法，因為應用程式衝突通常涉及排除目錄。您可以使用絕對路徑來建立路徑排除。在Windows上，還可以使用CSIDIL或KNOWNFOLDERID建立路徑排除。

例如，要在Windows上排除`Program Files`目錄中的AV應用程式，排除路徑可以是以下任意路徑：

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



注意：路徑排除項是遞迴的，並排除所有子目錄。

部分路徑匹配（僅限Windows）

如果路徑排除中未提供尾隨斜線，則Windows聯結器會在路徑上執行部分匹配。Mac和Linux不支援部分路徑匹配。

例如，如果您在Windows上套用下列「路徑」排除專案：

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

則會排除下列所有路徑：

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

將排除項從"C:\test"更改為"C:\test\"將阻止"C:\test123"被排除。

副檔名排除

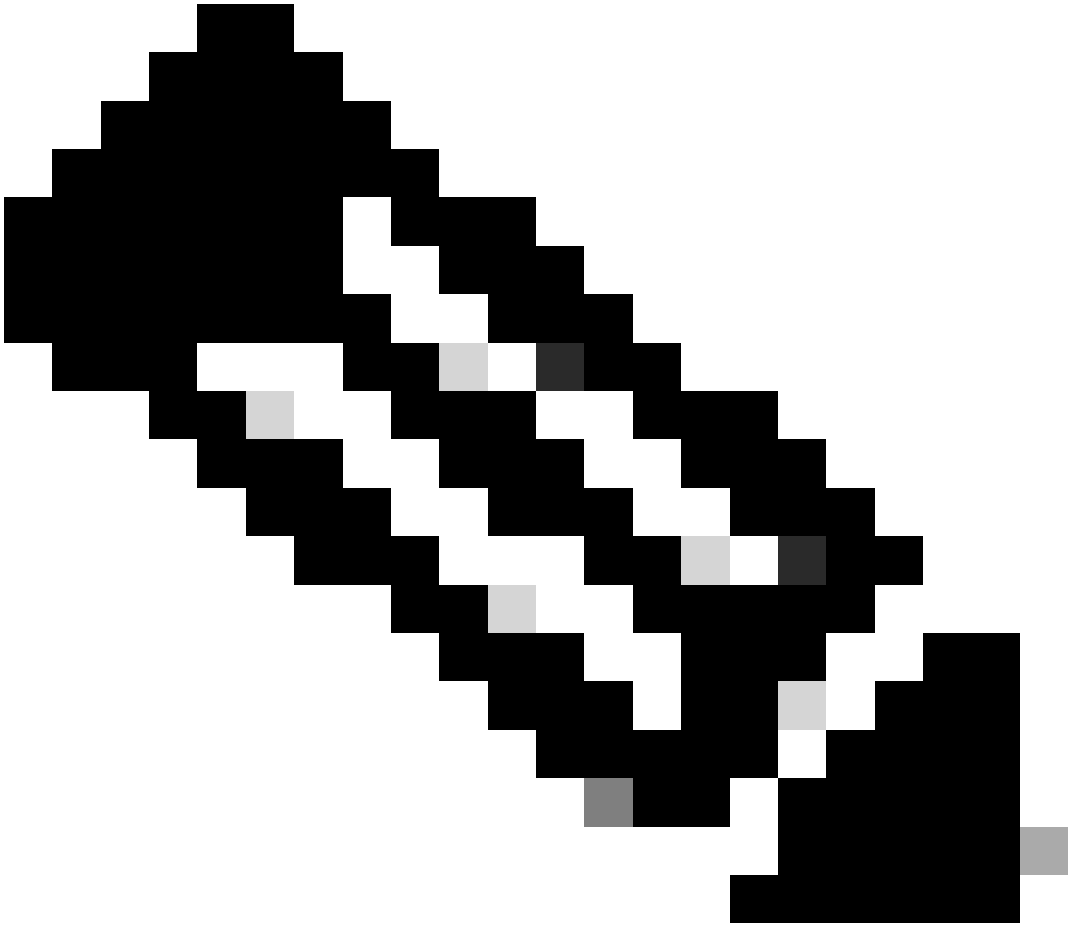
副檔名排除允許排除具有特定副檔名的所有檔案。

重點：

- 安全終結點控制檯中的預期輸入為.extension
- 如果沒有增加任何副檔名，Secure Endpoint Console會自動在副檔名前加上一個句點。
- 副檔名不區分大小寫。

例如，若要排除所有Microsoft Access資料庫檔案，您可以建立下列排除：

```
.MDB
```



注意：預設清單中提供了標準副檔名排除項，不建議刪除這些排除項，這樣做可能導致終端的效能變化。

萬用字元排除

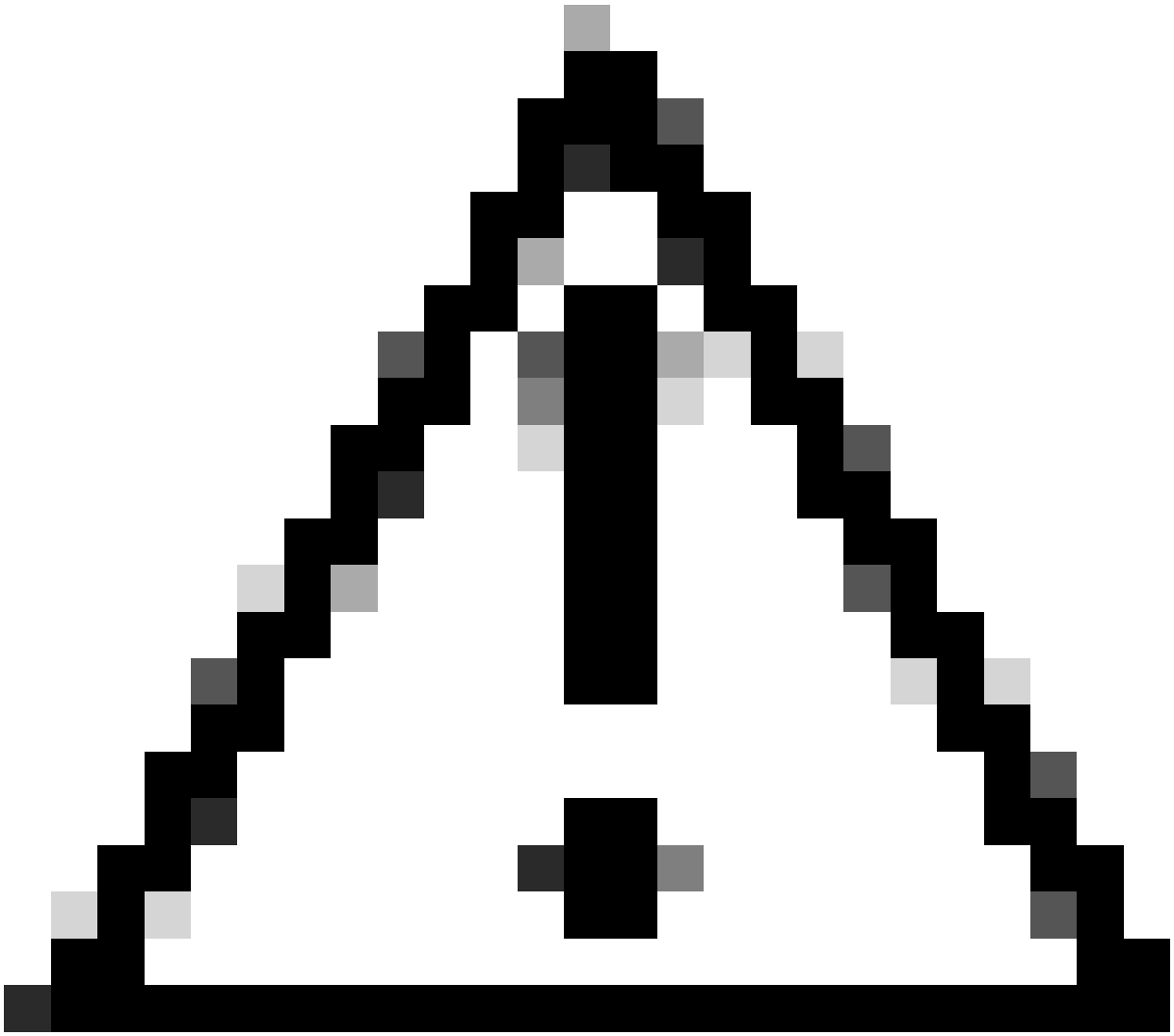
萬用字元排除項與「路徑」或「檔案副檔名」排除項相同，不同之處在於您可以使用星號字元(*)來表示路徑或副檔名中的萬用字元。

例如，如果您想將您在macOS上的虛擬機器排除在掃描之外，可以輸入以下路徑排除：

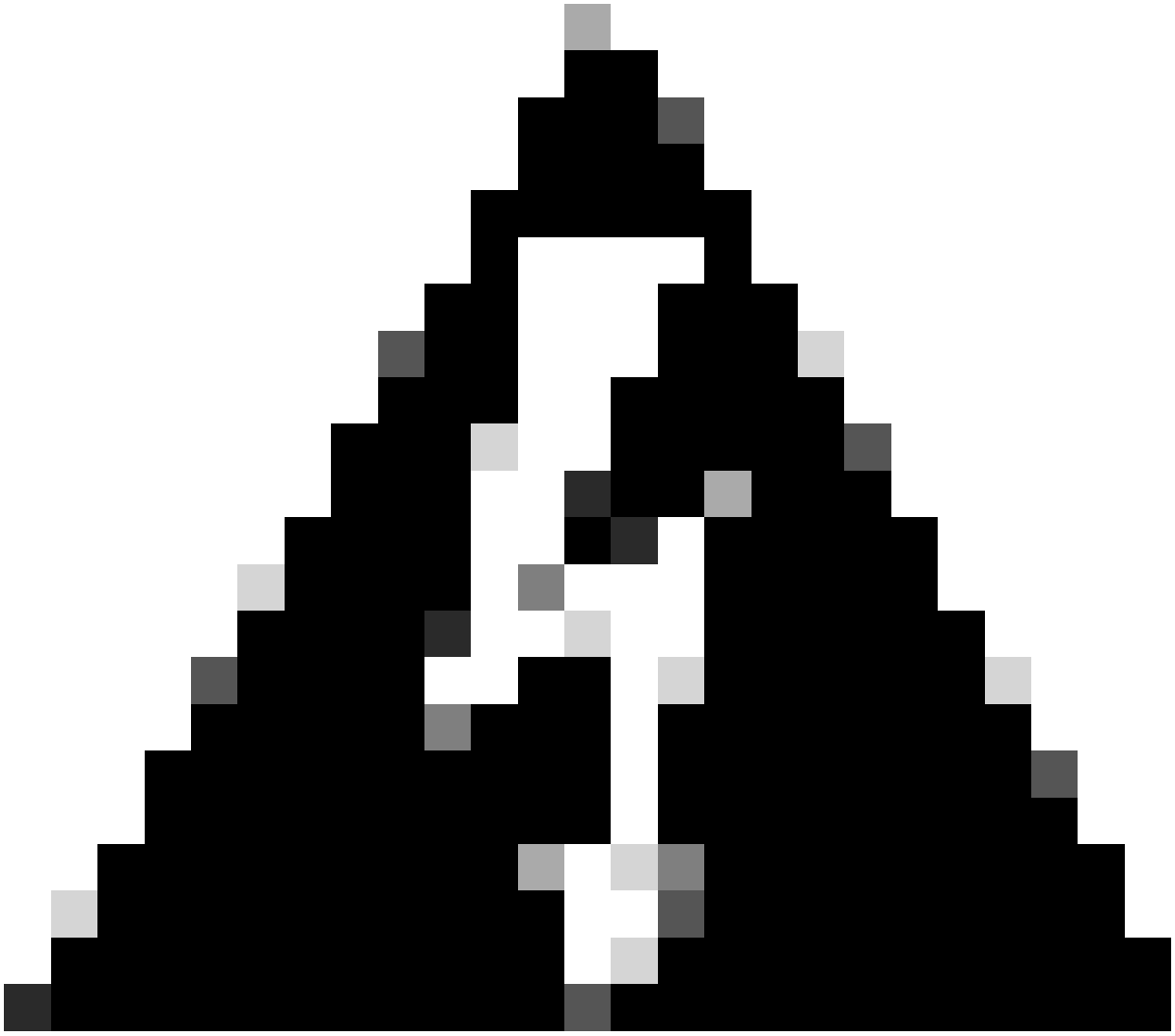
```
/Users/johndoe/Documents/Virtual Machines/
```

但是，此排除將只適用於一個使用者，因此請以星號替換路徑中的使用者名稱，並建立萬用字元排除以排除所有使用者的此目錄：

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



注意：萬用字元排除不會止於路徑分隔符，這可能會導致意外排除。例如，`exampleC:\*\test` excludesC:\sample\test以及`C:\1\test**` 或C:\sample\test123。



警告：以星號字元開始排除可能會導致嚴重的效能問題。移除或變更所有以星號字元開頭的排除專案，以減輕CPU的影響。

Windows

在Windows上建立萬用字元排除時，有一個選項可套用至所有磁碟機代號。選取此選項會將萬用字元排除套用至所有已掛載的磁碟機。

如果您手工建立相同的排除規則，則需要在它前面加上^[A-Za-z]，例如：

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

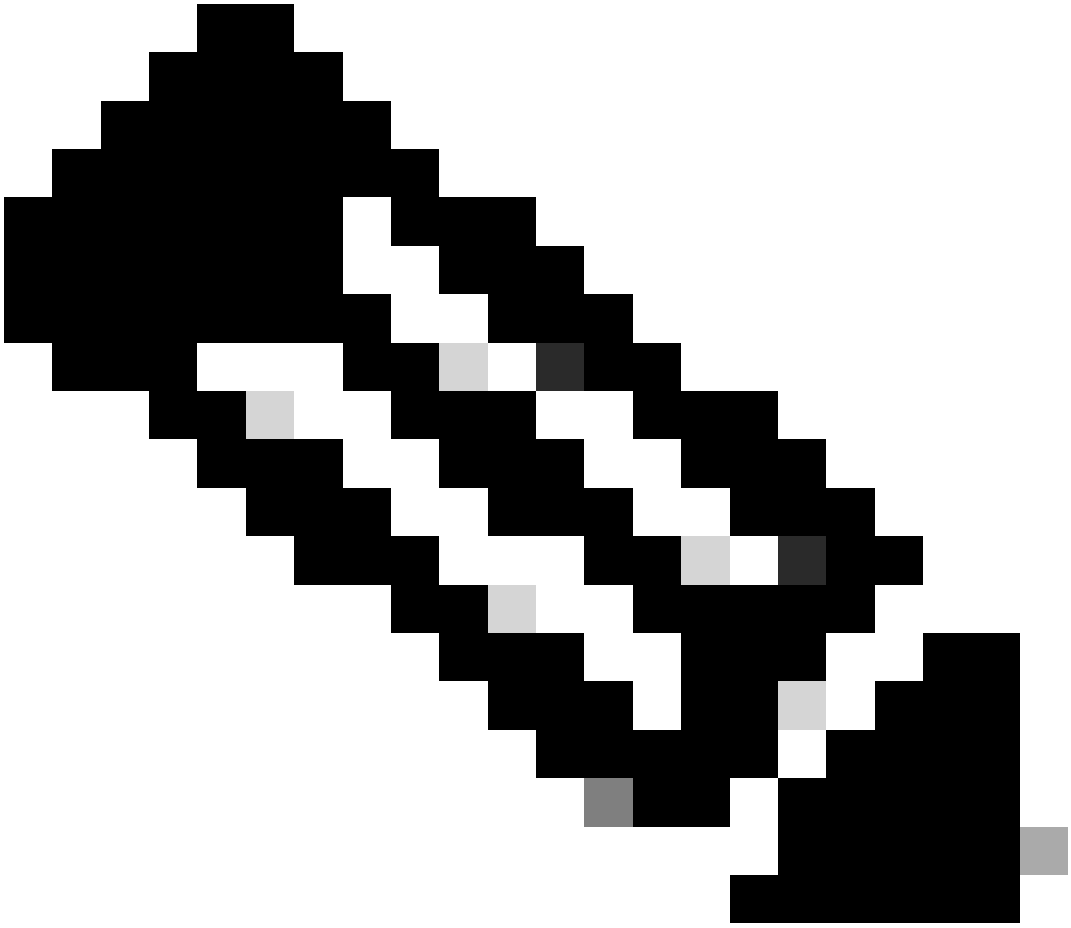
在這兩個示例中，都將排除C:\testpath和D:\testpath。

如果為萬用字元排除選擇`Apply to all drive letters`，安全終端控制檯將自動生成`^[A-Za-z]`。

可執行檔排除（僅限Windows）

執行檔排除項僅適用於啟用防攻擊的Windows聯結器。執行檔排除會排除某些執行檔，使其不受利用漏洞防護的保護。只有在遇到問題或效能問題時，才應該將執行檔從防漏洞攻擊中排除。

您可以檢查受保護的進程清單，並透過在應用程式排除欄位中指定其執行檔名，將任何進程從保護中排除。可執行檔排除必須與`name.exe`格式的執行檔名稱完全相符。不支援萬用字元。

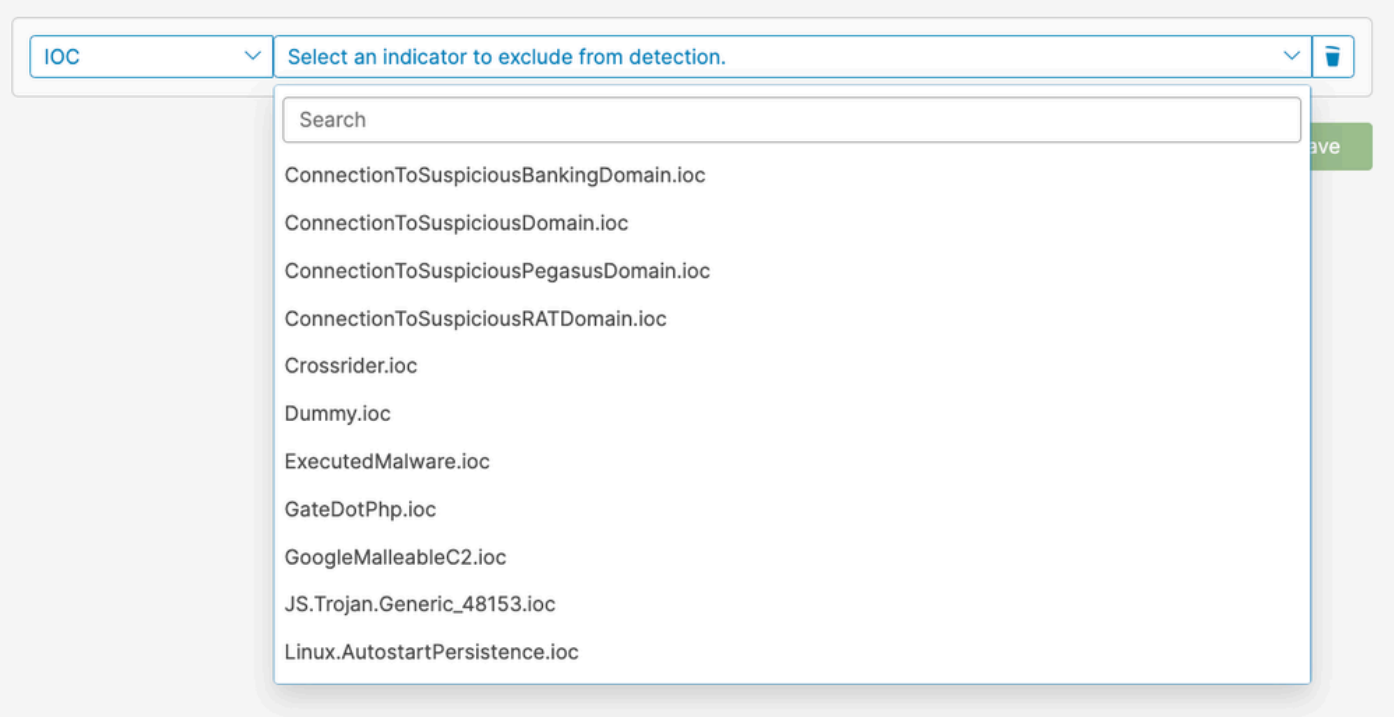


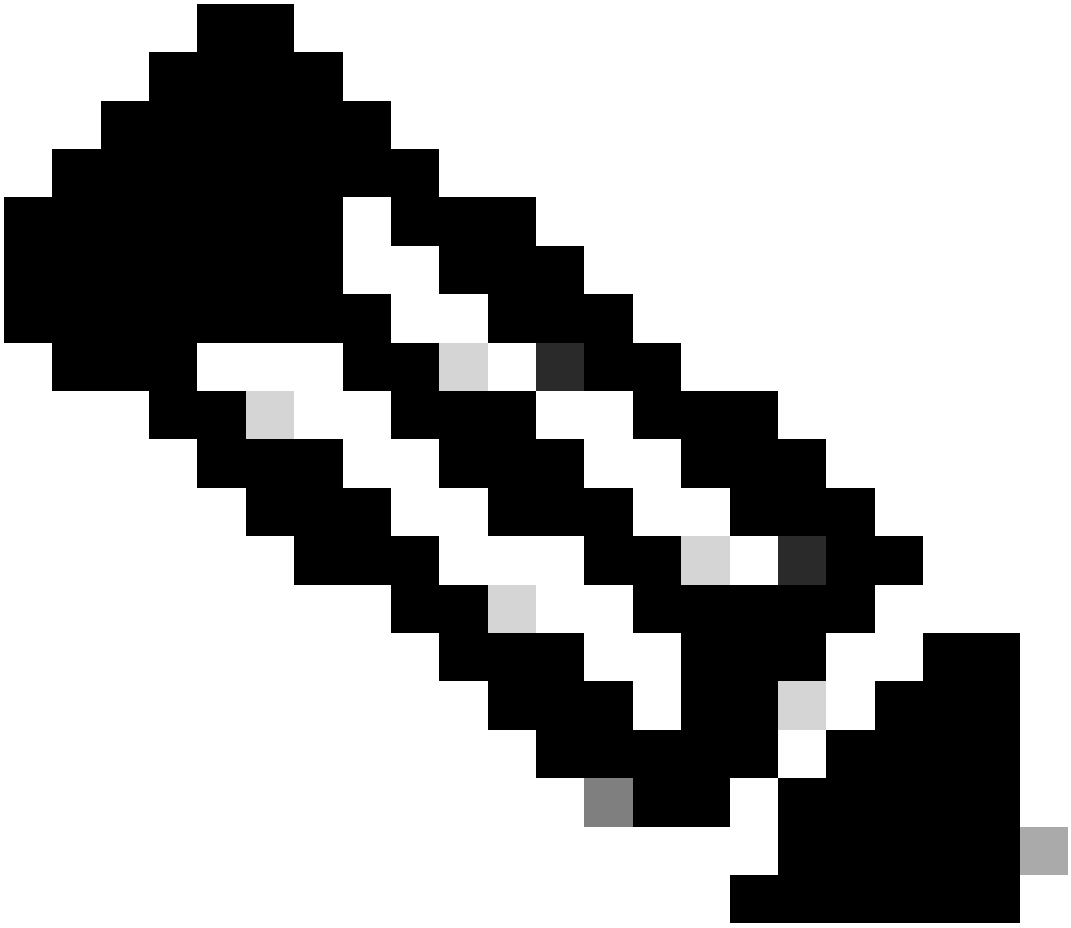
> 注意：只有應用程式才能通過安全終端控制檯使用可執行排除項排除。任何與DLL相關的排除都需要打開支援案例才能建立排除。

找到正確的漏洞防禦排除項是一個比其他任何排除型別都要密集得多的過程，需要進行大量測試以最大限度地減少任何有害的安全漏洞。

IOC排除（僅限Windows）

IOC排除允許排除雲危害表現。如果自定義或內部應用程式可能未簽名，導致某些IOC頻繁觸發，則此功能非常有用。Secure Endpoint Console提供一份指示器清單，供您從IOC排除中進行選擇。您可以透過下拉式清單選取要排除的指標：





注意：如果排除嚴重性高或嚴重的IOC，您將無法檢視它，並可能使您的組織面臨風險。只有在遇到大量誤報檢測時，才應排除這些IOC。

CSIDL與KNOWNFOLDERID（僅限Windows）

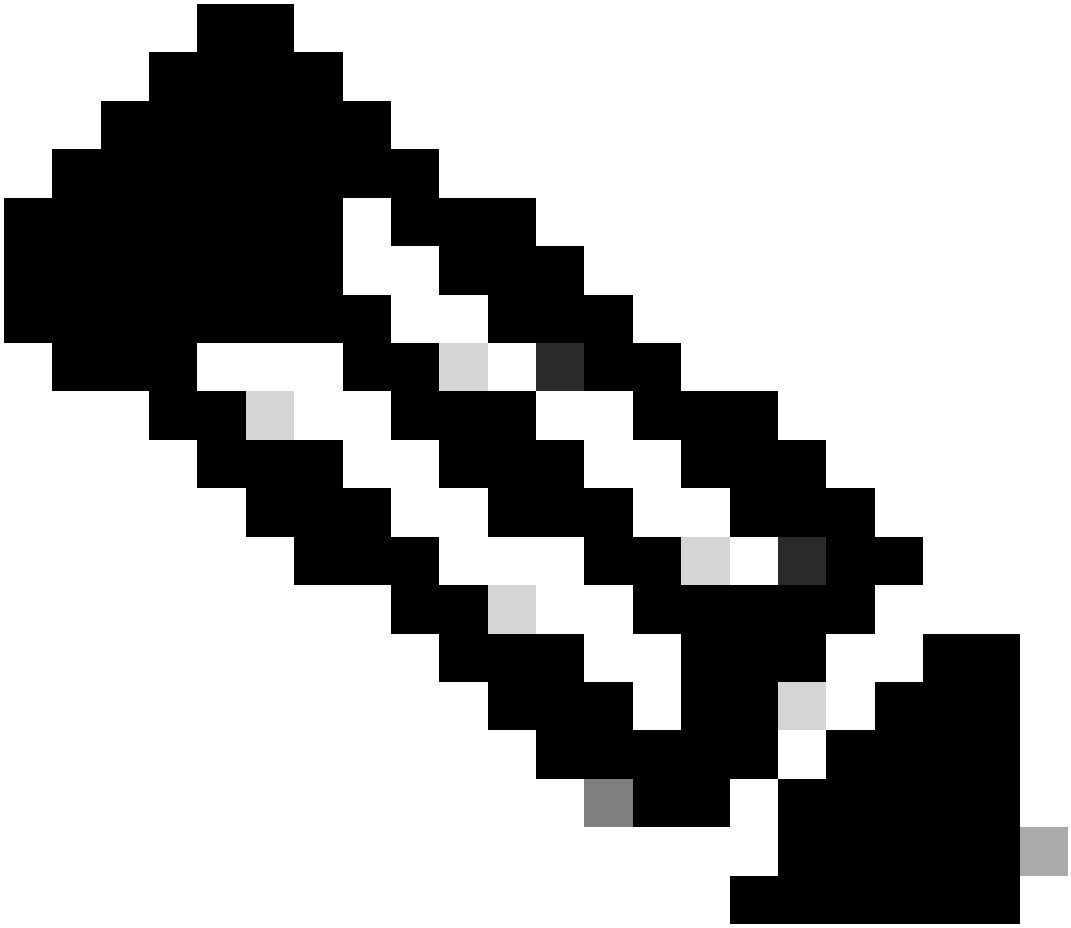
在編寫Windows的路徑和進程排除項時，接受並鼓勵使用CSIDL和KNOWNFOLDERID值。CSIDL/KNOWNFOLDERID值對於使用替代磁碟機代號的環境建立程式與路徑排除項很有用。

在使用CSIDL/KNOWNFOLDERID時，需要考慮一些限制。如果您的環境在一個以上的磁碟機代號上安裝程式，則CSIDL/KNOWNFOLDERID值只會參照標示為預設或已知安裝位置的磁碟機。

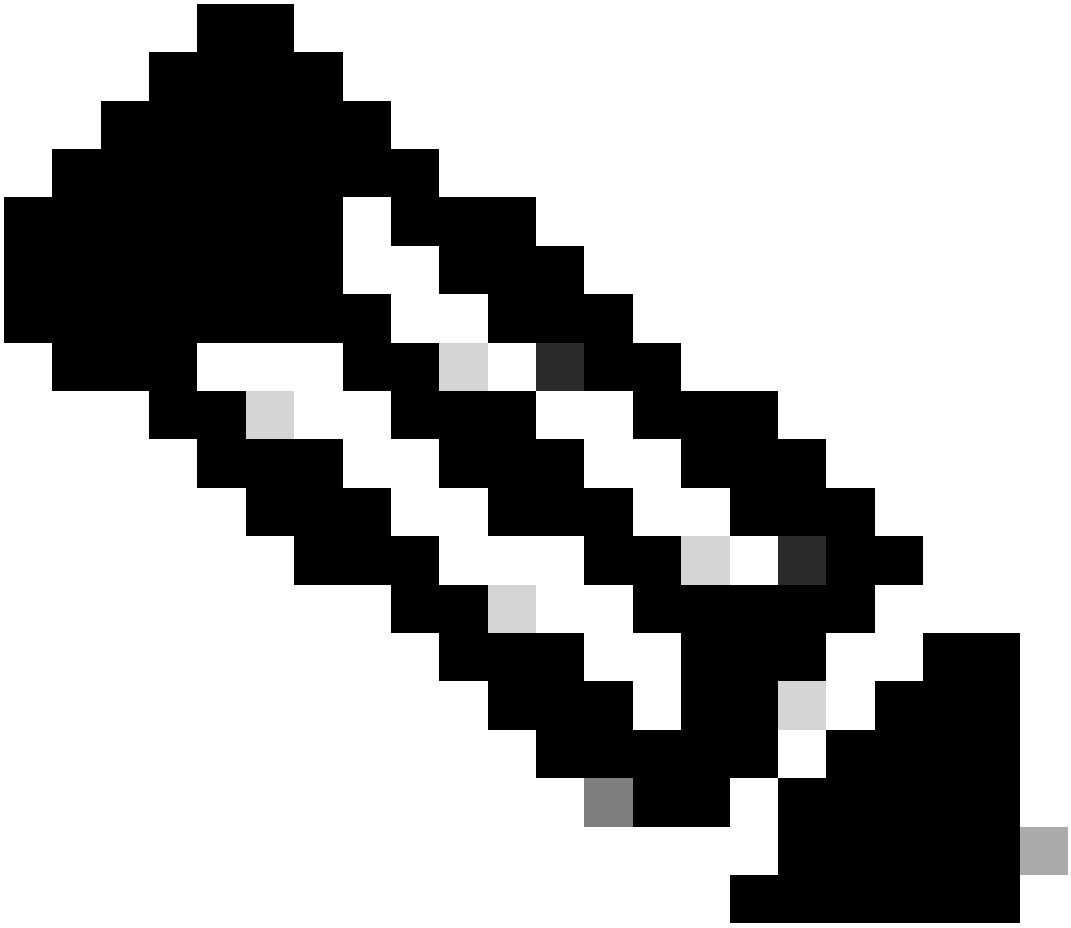
例如，如果作業系統安裝在C:\上，但Microsoft SQL的安裝路徑已手動更改為D:\，則已維護的排除清單中的基於CSIDL/KNOWNFOLDERID的排除不適用於該路徑。這意味著對於不在C:\驅動器上的每個路徑或進程排除必須輸入一個排除，因為使用CSIDL/KNOWNFOLDERID不會對映它。

有關詳細資訊，請參閱以下Windows文檔：

- CSIDL
- KNOWNFOLDERID



注意：僅Windows聯結器8.1.7及更高版本支援KNOWNFOLDERID。舊版的Windows聯結器使用CSIDL值。



注意：KNOWNFOLDERID值區分大小寫。例如，您必須使用valueFOLDERID_ProgramFiles而不是無效的valueFolderID_programfiles。

準備聯結器以進行排除調整

若要準備聯結器以進行排除調整，您需要：

1. 設定要在調試模式下運行的策略和組。
2. 根據正常業務操作運行新Debug組中的電腦，並留出時間獲取足夠的聯結器日誌資料。
3. 產生聯結器上的診斷資料，以用來辨識排除。

有關啟用調試模式和收集不同作業系統上的診斷資料的說明，請參閱以下文檔：

- 適用於Mac診斷資料收集的Cisco安全端點聯結器
- 適用於Linux診斷資料收集的Cisco安全端點聯結器
- 分析高CPU的AMP診斷套件(Windows)

辨識排除

MacOS和Linux

在調試模式下生成的診斷資料提供了兩個可用於建立排除的檔案：fileops.txt和execs.txt。fileops.txt檔案可用於建立路徑/副檔名/萬用字元排除，execs.txt檔案可用於建立進程排除。

建立處理序排除

execs.txt檔案列出觸發Secure Endpoint執行檔案掃描的可執行路徑。每個路徑都有相關的計數，指示掃描的次數，並且清單會以遞減順序排序。您可以使用此清單來判斷執行事件數量龐大的處理序，然後使用處理序路徑來建立排除專案。但是，不建議排除一般公用程式（例如/usr/bin/grep）或解譯器（例如/usr/bin/ruby）。如果一般公用程式或解譯器產生大量的檔案掃描，您可以執行更多調查來嘗試和建立更有針對性的排除專案：

1. 排除父進程：確定哪個應用程式正在執行該進程（例如，查詢正在執行grep的父進程）並排除此父進程。若且唯若父進程可以安全地變為進程排除時，應執行此操作。如果父項排除套用至子項，則來自父項處理作業的任何子項呼叫也會被排除。
2. 排除指定使用者的程式：決定執行程式的使用者。如果某個特定使用者正在大量執行進程，則可以僅為該特定使用者排除該進程（例如，如果某個進程正被使用者「root」以大量呼叫時，您可以排除該進程，但僅針對指定的使用者「root」，這將允許安全終端監控非「root」的任何使用者執行給定進程）。

execs.txt的示例輸出：

```
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
```

建立路徑、副檔名和萬用字元排除

fileops.txt檔案列出了檔案建立、修改和重新命名活動觸發「安全終端」執行檔案掃描的路徑。每個路徑都有相關的計數，指示掃描的次數，並且清單會以遞減順序排序。開始使用路徑排除的一個方法是，從fileops.txt中查詢最常掃描的檔案和資料夾路徑，然後考慮為這些路徑建立規則。雖然高計數並不一定意味著必須排除路徑（例如，可以經常掃描儲存電子郵件的目錄，但不能排除該目錄），但清單提供了辨識排除候選目錄的起點。

fileops.txt的示例輸出：

```
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
```

一個好的經驗法則是，任何具有日誌或日誌副檔名的檔案都應被視為合適的排除候選。

行為保護引擎

行為保護引擎是在Linux聯結器1.22.0版和macOS聯結器1.24.0版中引入的；從這些版本開始，聯結器可以檢測到大量系統活動，然後引發故障18。

處理序排除會套用至所有引擎和檔案掃描。將進程排除應用於非常活躍的良性進程，以補救此故障。由Debug Mode診斷資料生成的top.txt檔案可用於確定系統中最活躍的進程。有關詳細的修正步驟，請參閱安全終端Mac/Linux聯結器故障18指南。

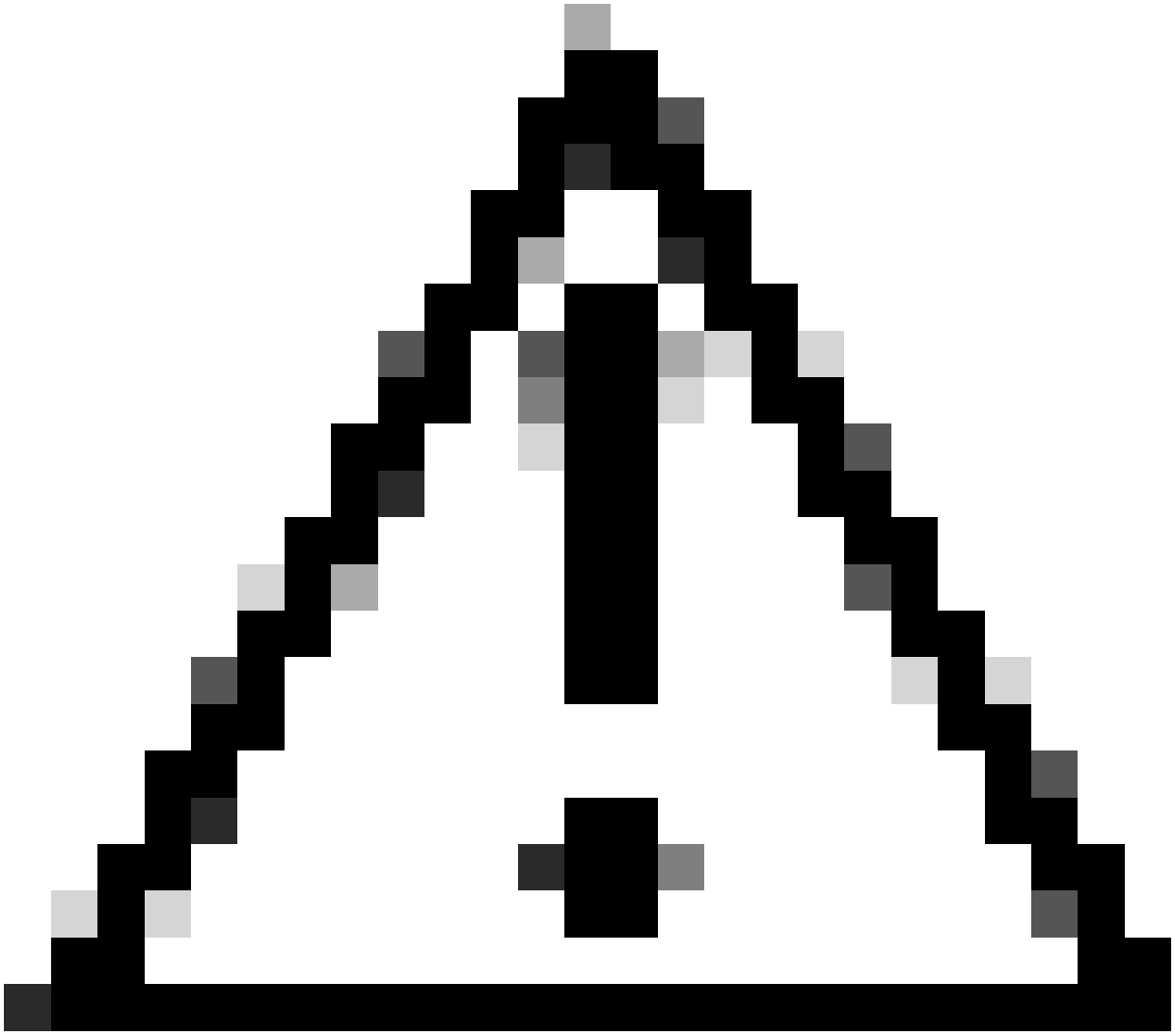
此外，進程排除可以阻止良性軟體的誤報行為保護檢測。對於Secure Endpoint Console中的誤報檢測，可以排除該進程以改進報告。

Windows

Windows作業系統較為複雜，因為父項與子項處理序的關係，所以有更多排除選項可供使用。這表示需要更深入的審閱，以辨識已經存取的檔案，以及產生這些檔案的程式。

有關使用安全端點分析和最佳化Windows效能的詳細資訊，請參閱思科安全部GitHub頁的此Windows調整工具。

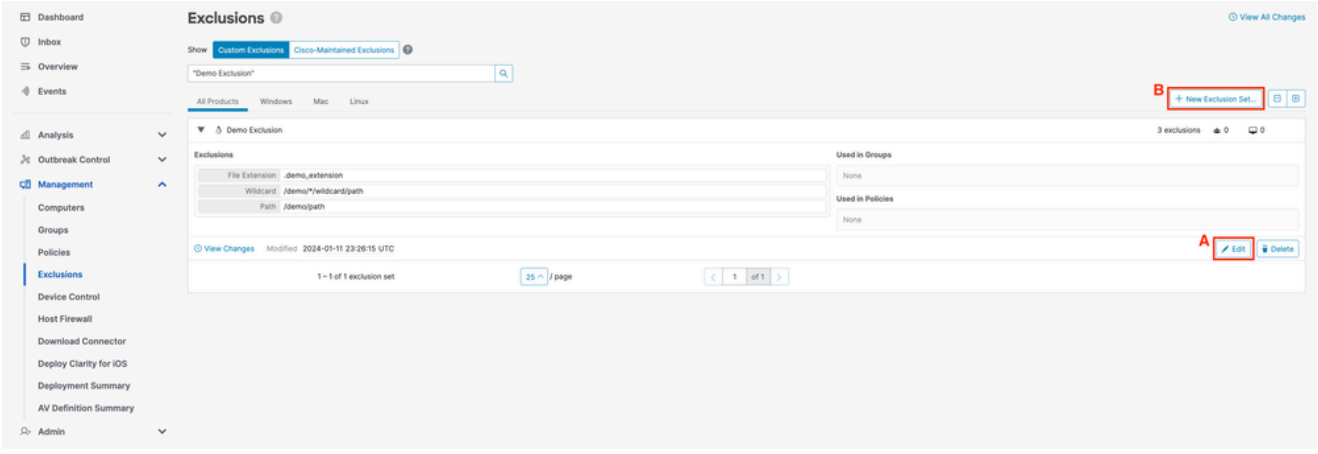
在安全終端控制檯中建立排除規則



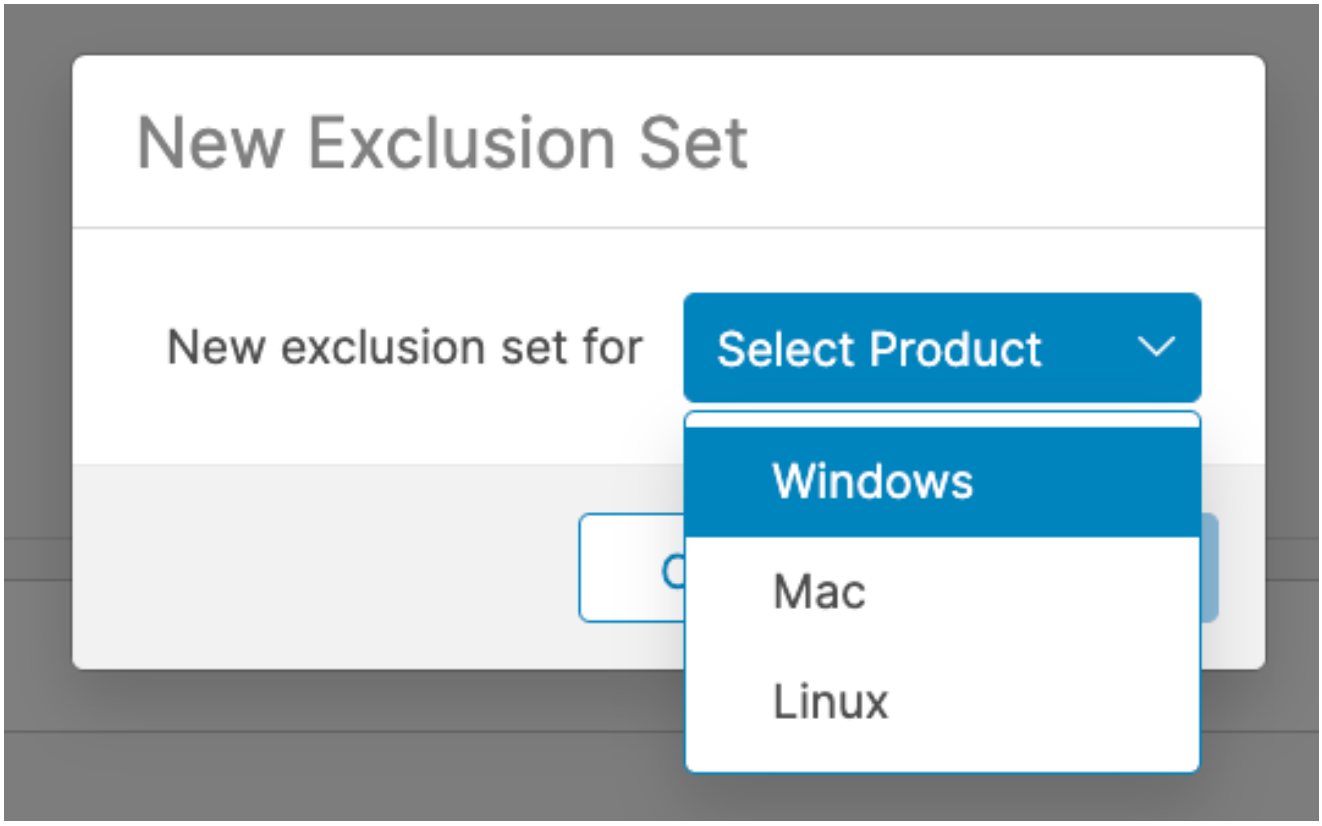
注意：在寫入排除命令之前始終瞭解檔案和進程，以避免終端上的安全漏洞。

完成以下步驟，使用Secure Endpoint Console建立新的排除規則：

1. 在Secure Endpoint Console中，透過選擇`Management` -> `Exclusions`導航到「Policies」頁。(A)找到您要修改的排除集，然後按一下`Edit`，或者(B)按一下`+New Exclusion Set...`。

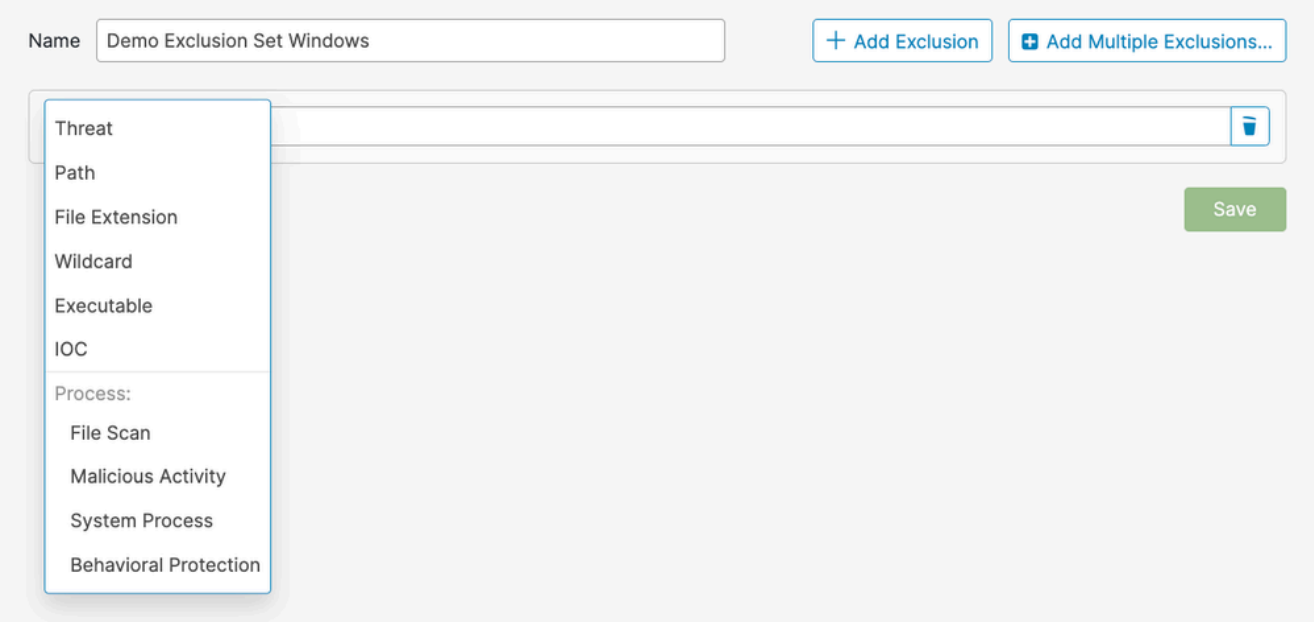


2. 在新建排除集彈出窗口中，選擇要為其建立排除集的作業系統。按一下Create。

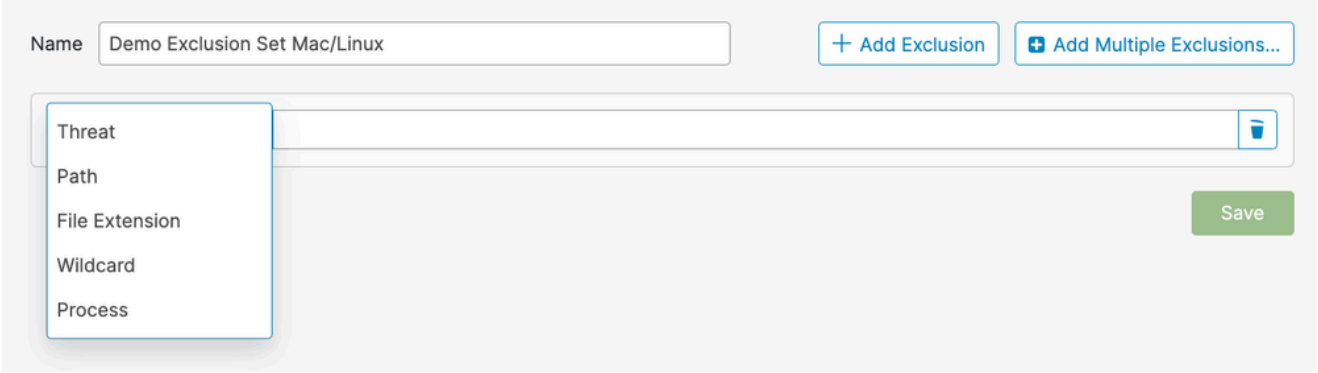


3. 您將被重定向到新的排除集頁面。按一下+ Add Exclusion，然後從Select Type下拉選單中選擇排除型別。

Windows:



Mac/Linux：



4. 填寫所選排除型別的必填欄位。
5. 重複步驟2和3以增加更多規則，或按一下Save儲存排除集。

最佳實務

建立排除項時應小心，因為它們會降低思科安全終端提供的保護級別。排除的檔案在快取或雲中未被雜湊處理、掃描或可用，活動未被監控，後端引擎、裝置軌跡和高級分析中缺少資訊。

排除項只能用於目標例項，例如特定應用程式的相容性問題或效能問題，否則無法改進。

建立排除項時應遵循的一些最佳實踐包括：

- 僅針對已證實的問題建立排除專案
  - 不要假定排除是必需的，除非已證明這是一個無法通過其他方法解決的問題。
  - 在應用排除之前，必須徹底調查和緩解效能問題、誤報或應用程式相容性問題。
- 優先使用處理序排除項而非路徑/檔案副檔名/萬用字元排除項
  - 與使用路徑、副檔名和萬用字元排除組合來達到相同結果相比，進程排除提供了一種更直接的方法來排除良性軟體活動。
  - 建議儘可能以對應的程式排除項替換目標程式執行檔的路徑、副檔名和萬用字元排除項。
- 避免廣泛排除
  - 不要排除終端的大部分，例如整個C驅動器。
  - 使用檔案的完整路徑，而不只是檔案名稱。
  - 使用Device Trajectory、Secure Endpoint Diagnostics Data和Windows Tuning Tool調查和確定特定排除情況。
- 避免過度使用萬用字元排除
  - 使用萬用字元建立排除專案時要小心。儘可能使用更具體的排除項。
  - 使用排除中的萬用字元數量下限；只有真正可變的資料夾才應使用萬用字元。
- 避免排除一般公用程式和口譯人員
  - 不建議排除一般公用程式或口譯人員。
  - 如果您確實需要排除一般公用程式或解譯器，請提供一個程式使用者（僅限macOS/Linux）。
  - 例如，避免編寫包括python、`java`、`ruby`、`bash`、`sh`等在內的排除檔案。
- 避免重複排除
  - 建立排除之前，請檢查該排除項是否已經存在於自定義排除項或思科維護的排除項中。
  - 刪除重複排除可提高效能並減少對排除的操作管理。
  - 確定路徑/副檔名/萬用字元排除未涵蓋在程式排除中指定的路徑。

- 避免排除已知常用於惡意軟體攻擊的進程
  - 有關詳細資訊，請參閱不建議排除。
- 移除過時的排除專案
  - 定期審查和審計您的排除清單，並記錄增加某些排除的原因。
- 在危害時刪除排除項
  - 當聯結器受到威脅時，必須刪除排除項，以便重新獲得最佳安全性和可視性。
  - 自動操作可用於在感染後對聯結器應用更安全的策略。如果聯結器受到威脅，應將其移至包含策略的組，且不排除任何威脅，以確保應用最高級別的保護。
  - 有關如何主動設定「在受到侵害時移動電腦到組」自動操作的詳細資訊，請參閱辨識在安全終端中觸發自動操作的條件。
- 增加排除專案的保護
  - 當排除絕對必要時，請考慮可以採取什麼緩解策略，例如啟用防寫為排除的專案增加一些保護層。
- 智慧地建立排除
  - 透過選擇可唯一辨識要排除之應用程式的最高層級父項處理作業，來最佳化規則，並使用`套用至子項處理作業`選項來最小化規則數目。
- 從不排除啟動過程
  - 啟動進程(在macOS上為`launchd`、在Linux上為`init`或`systemd`)負責啟動系統上的所有其它進程，該進程位於進程階層的頂部。
  - 排除啟動進程及其所有子進程將有效地停用安全終端監控。
- 儘可能指定程式使用者（僅限macOS/Linux）
  - 如果使用者欄位留空，則排除將應用於運行指定程式的任何進程。
  - 雖然適用於任何使用者的排除更為靈活，但此廣泛範圍可能會無意中排除必須監控的活動。
  - 對於應用於共用程式(如運行時引擎(例如，`java`)和指令碼解釋程式(例如，`bash`、`python`))的規則，指定使用者尤其重要。
  - 指定使用者可限制範圍，並指示安全端點在監控其他例項時忽略特定例項。

不建議的排除專案

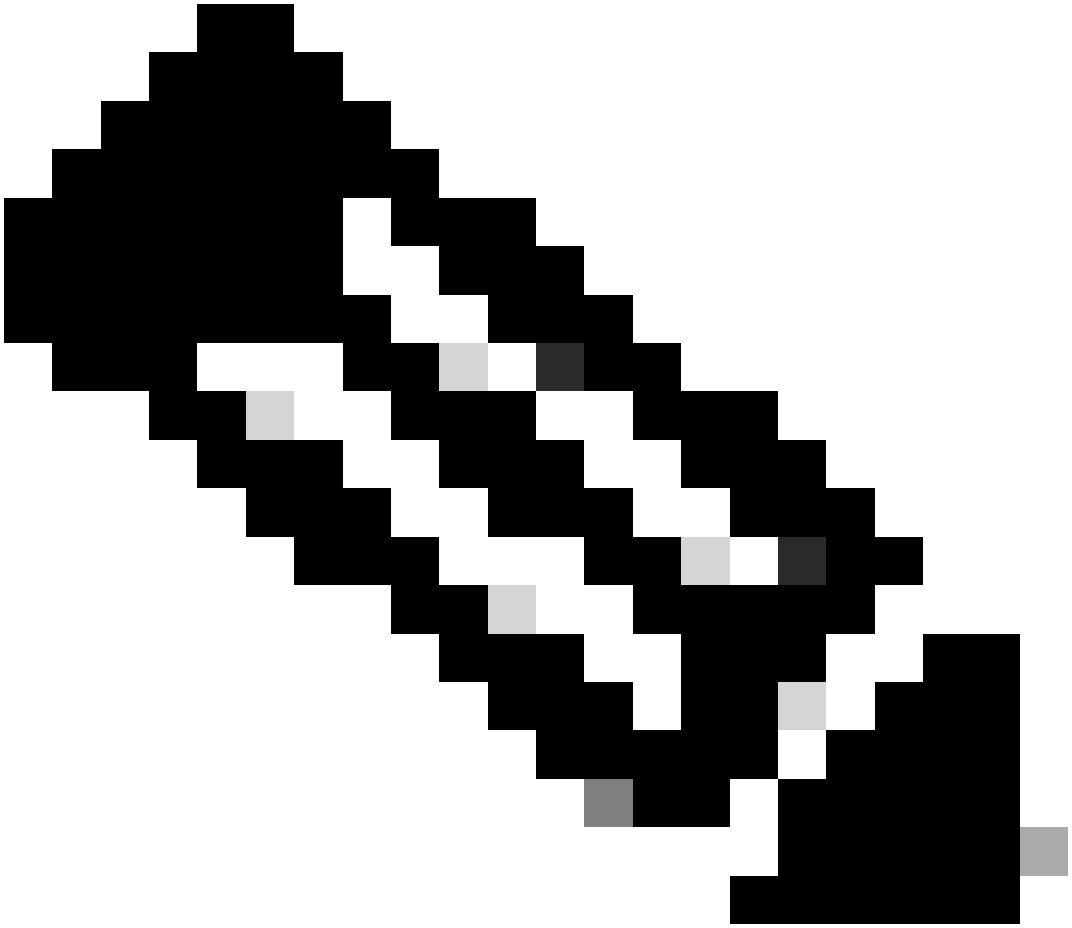
儘管不可能知道敵方可能使用的每種可能的攻擊媒介，但有一些核心攻擊媒介需要受到監控。為了保持良好的安全狀態和可視性，不建議使用以下排除項：

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
wuault.exe
.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
bash
java
python
python3
sh
zsh
/
/bin
/sbin
/usr/lib
思:
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檔案\<公司名稱>\
C:\Program檔案(x86)\<公司名稱>\
C:\Users\<UserProfileName>\AppData\Local\Temp\
C:\Users\<UserProfileName>\AppData\LocalLow\Temp\



注意：這不是要避免的詳盡的排除清單，但可以深入瞭解核心攻擊媒介。保持對這些路徑、副檔名和進程的可視性至關重要。

相關資訊

- 技術支援與文件 - Cisco Systems
- 思科安全終端- TechNotes
- 思科安全終端-使用手冊
- 排除安全端點中的漏洞攻擊預防故障
- 確定在安全終端中觸發自動操作的條件

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。