セキュアエンドポイントの除外の設定と特定

内容

はじめに

このドキュメントでは、除外の概要、除外を特定する方法、およびCisco Secure Endpointで除外を作成するためのベストプラクティスについて説明します。

免責事項

このドキュメントの情報は、Windows、Linux、およびmacOSオペレーティングシステムに基づ

くものです。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

概要

このドキュメントを読むと、次の項目を理解できます。

- 除外とは何か、およびCisco Secure Endpointで使用可能なさまざまなタイプの除外について説明します。
- 除外チューニング用にコネクタを準備する方法
- 強力な可能性がある除外を特定する方法
- Cisco Secure Endpoint Consoleで新しい除外を作成する方法
- 除外を作成するためのベストプラクティス

除外の概要

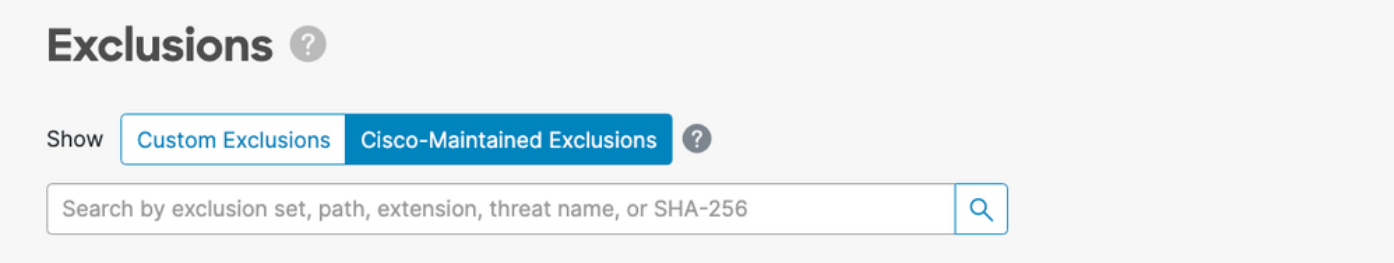
除外セットとは、コネクタでスキャンや処罰を行わないようにするディレクトリ、ファイル拡張子、ファイルパス、プロセス、脅威の名前、アプリケーション、または侵入の痕跡(indicators of compromise)のリストです。Secure Endpointなどのエンドポイント保護を有効にした場合は、マシンのパフォーマンスとセキュリティのバランスを保つために、除外を慎重に作成する必要があります。この記事では、Secure Endpoint Cloud、TETRA、SPP、およびMAPの除外について説明します。

厳格なポリシーからオープンなポリシーまで、あらゆる環境とそれを制御するエンティティはユニークです。したがって、除外は状況に応じて個別に調整する必要があります。

除外は、Cisco-Maintained除外とカスタム除外の2つの方法で分類できます。

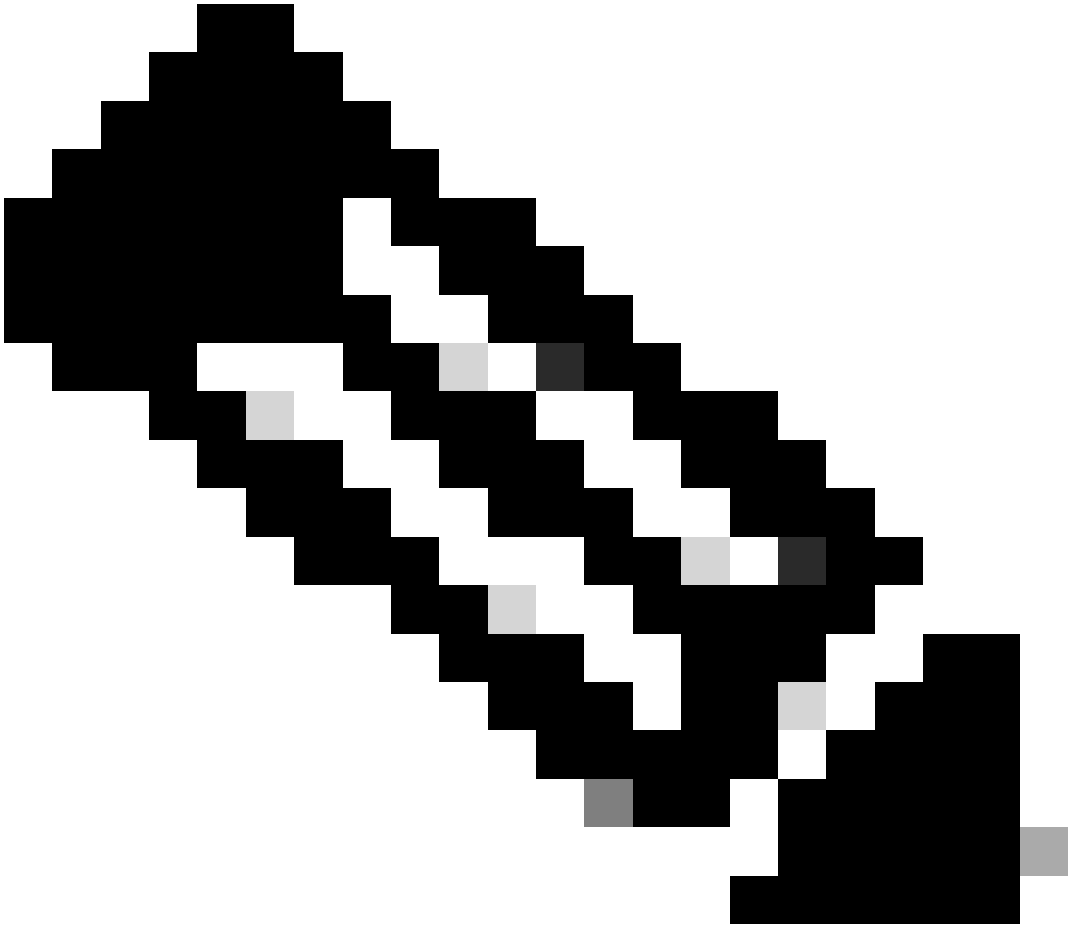
シスコが管理する除外

シスコが管理する除外は、調査に基づいて作成され、一般的に使用されるオペレーティングシステム、プログラム、およびその他のセキュリティソフトウェアで厳格なテストを受けた除外です。これらの除外を表示するには、`Exclusions`ページでSecure Endpoint Console（登録ユーザ専用）の`Cisco-Maintained Exclusions`を選択します。



シスコは、アンチウイルス(AV)ベンダーによって公開された推奨される除外リストを監視し、推

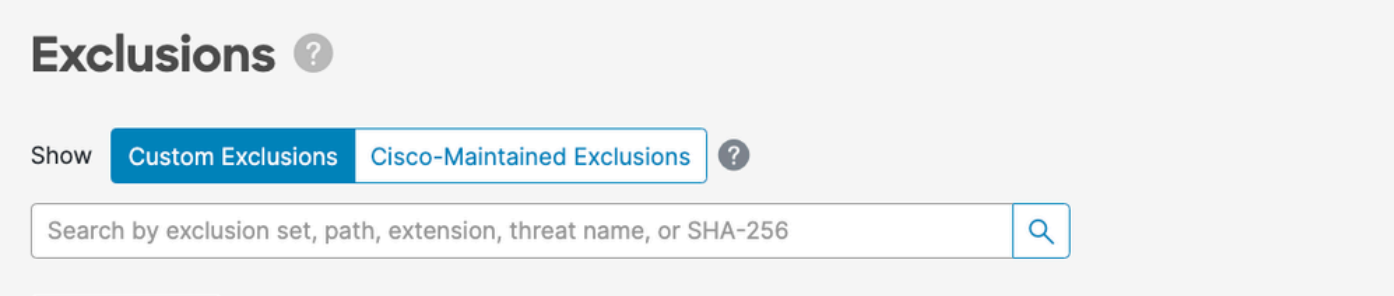
奨される除外を含むようにシスコが維持する除外を更新します。



注：一部のAVベンダーは、推奨される除外を公開しない場合があります。この場合、お客様はAVベンダーに問い合わせて推奨される除外リストを要求し、サポートケースをオープンしてCisco-Maintained除外リストを更新する必要があります。

カスタム除外

カスタム除外は、エンドポイントでのカスタム使用例のためにユーザが作成した除外です。除外された項目は、Secure Endpoint Consoleの`Exclusions`ページで`Custom Exclusions`を選択することで表示できます。



除外のタイプ

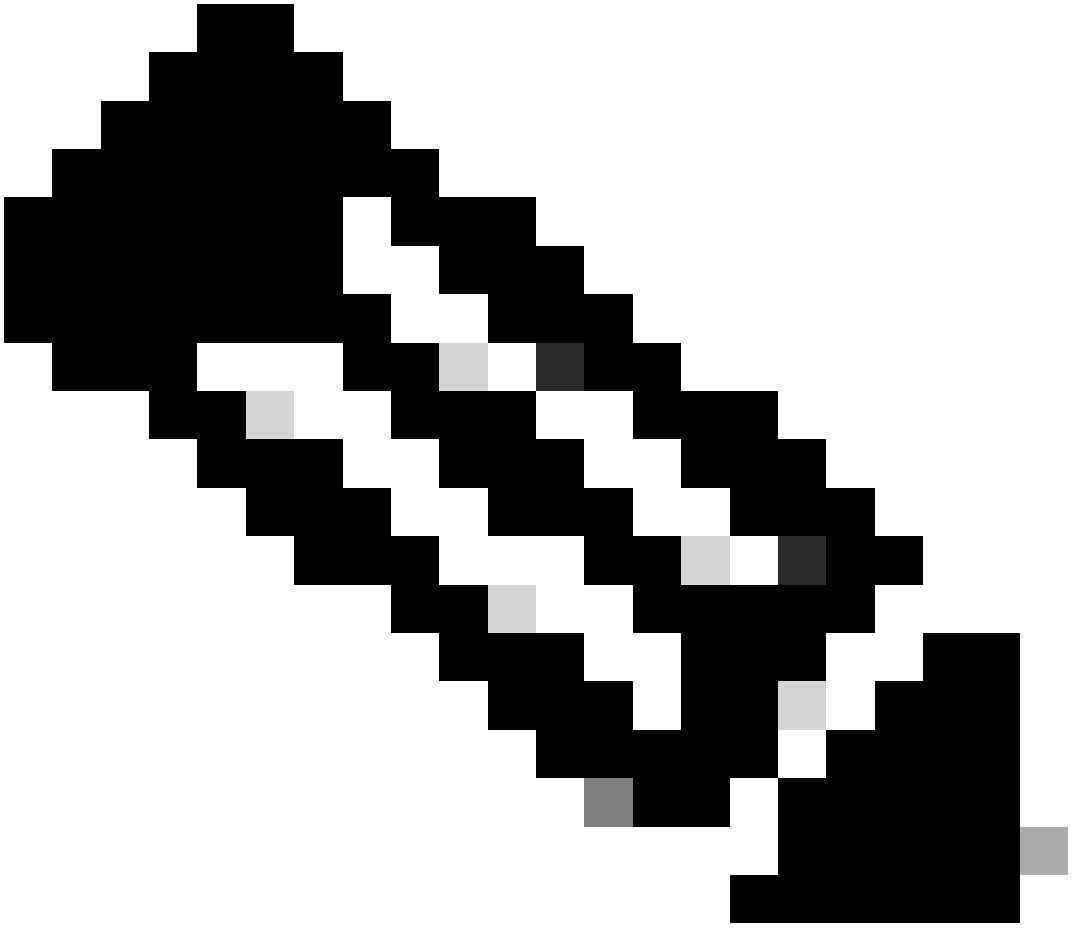
プロセスの除外

プロセスの除外により、管理者はサポートされているエンジンからプロセスを除外できます。次の表に、各プラットフォームでプロセス除外をサポートするエンジンの概要を示します。

オペレーティング システム	[Engine]			
	ファイルスキャン	システムプロセスの保護	悪意のあるアクティビティの保護	動作保護
Windows	✓	✓	✓	✓
Linux	✓	0.✗	0.✗	✓
MacOS	✓	0.✗	0.✗	✓

MacOSおよびLinux

プロセス除外を作成する場合は、絶対パスを指定する必要があります。オプションのユーザーを指定することもできます。パスとユーザーの両方を指定した場合、プロセスを除外するには両方の条件を満たす必要があります。ユーザーを指定しない場合は、プロセスの除外がすべてのユーザーに適用されます。



注:macOSおよびLinuxでは、プロセスの除外はすべてのエンジンに適用されます。

プロセスワイルドカード：

セキュアエンドポイントLinuxおよびmacOSコネクタは、プロセスの除外内でワイルドカードを使用してサポートします。これにより、除外される項目が少なく適用範囲が広くなりますが、定義されていない項目が多すぎる場合は危険です。ワイルドカードは、必要な除外を指定するために必要な最小文字数をカバーするためだけに使用する必要があります。

macOSおよびLinuxでのプロセスワイルドカードの使用：

- ワイルドカードは、1つのアスタリスク(*)を使用して表されます
- ワイルドカードは、単一文字またはディレクトリ全体の代わりに使用できます。
- パスの先頭にワイルドカードを配置することは無効と見なされます。
- ワイルドカードは、スラッシュまたは英数字の2つの定義済み文字の間で機能します。

例:

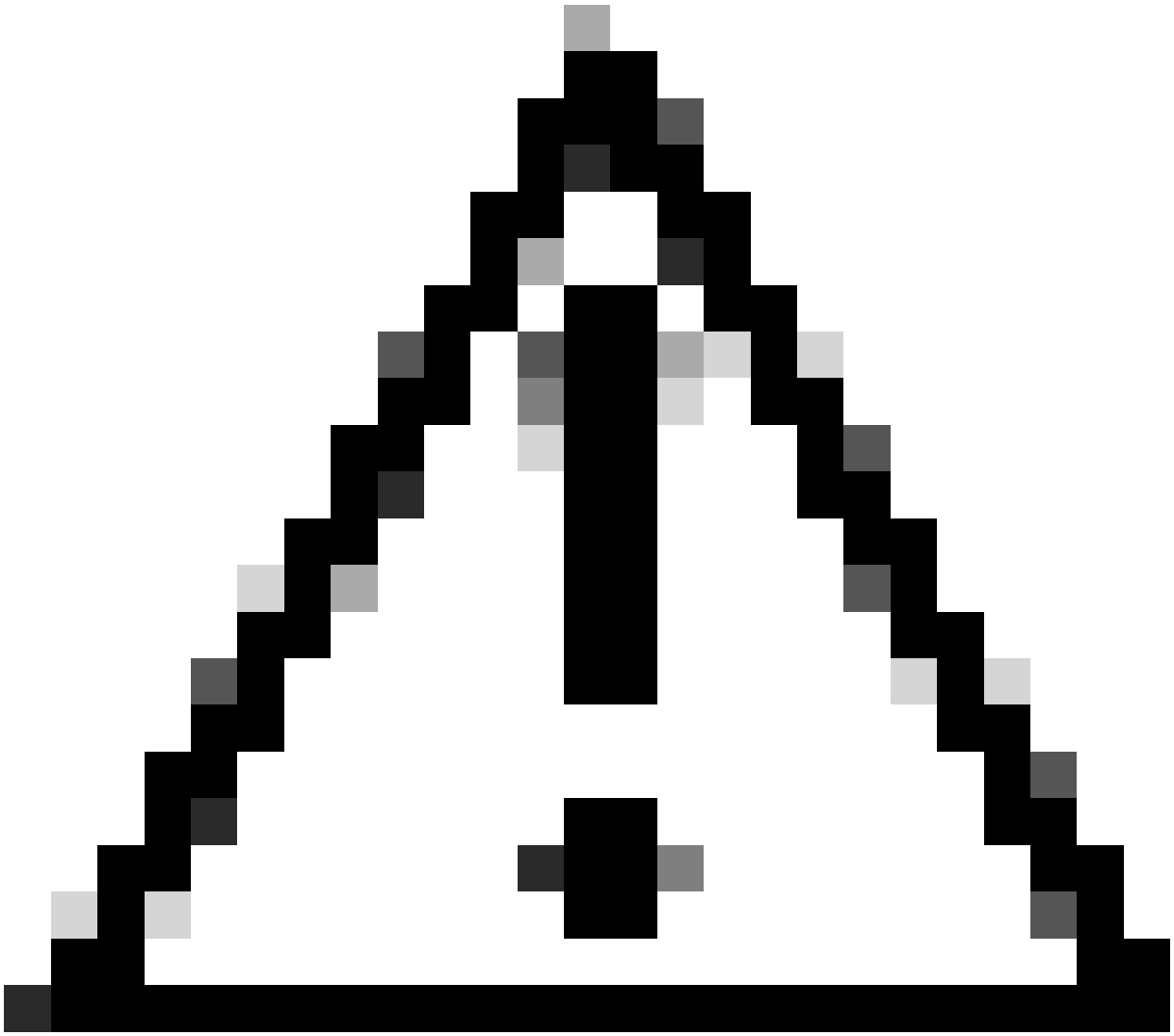
除外	予想される結果

/Library/Java/JavaVirtualMachines/*/java	JavaVirtualMachinesのすべてのサブフォルダ内のjavaを除外します。
/Library/Jibber/j*bber	jabber、jibber、jobberなどのプロセスを除外します。

Windows

プロセスの除外を作成する際に、プロセス実行可能ファイルの絶対パスまたはSHA-256を指定できます。パスとSHA-256の両方を指定した場合、プロセスを除外するには両方の条件を満たす必要があります。

Windowsでは、パス内でCSIDLまたはKNOWNFOLDERIDを使用して、プロセス除外を作成することもできます。

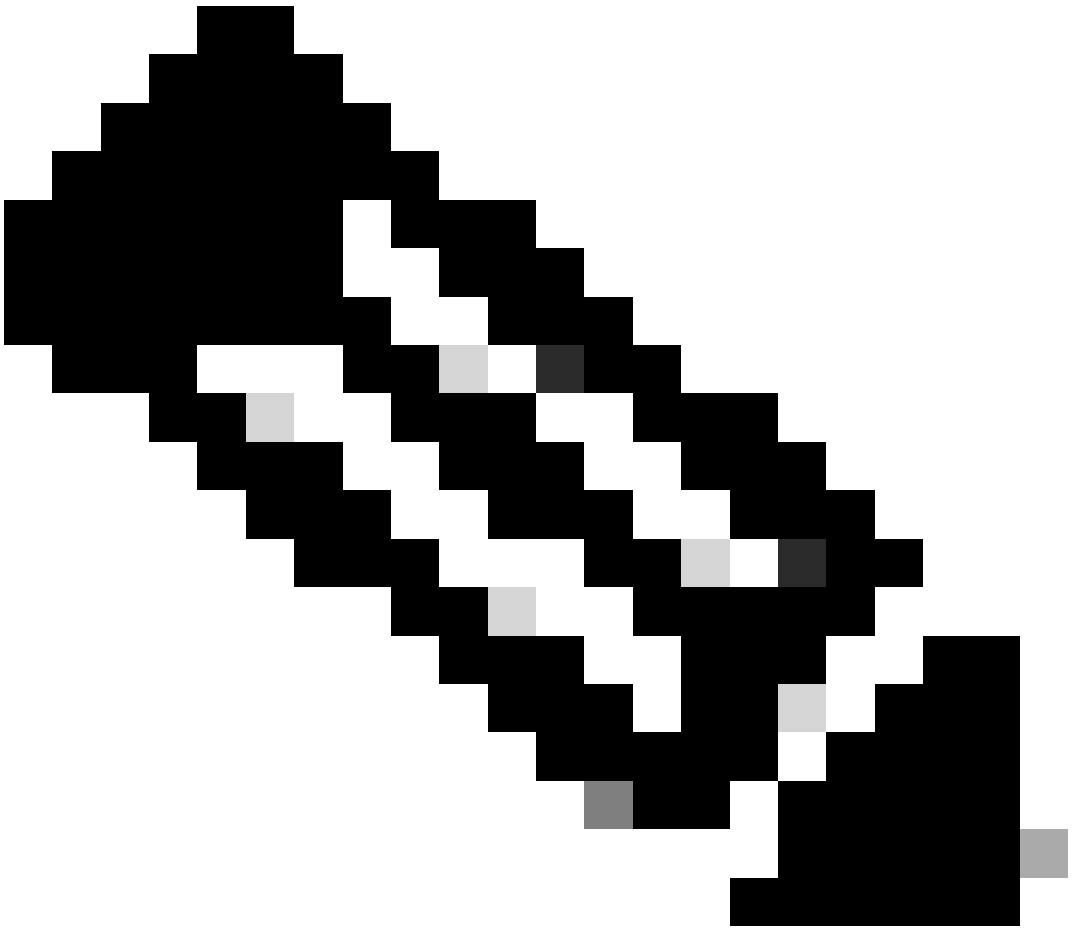


注意：除外されたプロセスによって作成された子プロセスは、デフォルトでは除外されません。プロセスの除外を作成するときに追加のプロセスを除外するには、子プロセスに適用を選択します。

制限：

- プロセスのファイルサイズ（バイト）がポリシーで設定されている最大スキャンファイルサイズよりも大きい場合、プロセスのSHA-256は計算されず、除外は機能しません。最大スキャンファイルサイズを超えるファイルには、パスベースのプロセス除外を使用します。
- Windowsコネクタでは、すべてのプロセス除外タイプで500のプロセス除外に制限があります。
    - プロセスの除外は、`policy.xml`のプロセス除外リストの先頭から、制限を超えてのみ有効です。
    - すべてのWindowsポリシーに`sfc.exe`のプロセス除外があります。これは、プロセス除外制限でカウントされます。

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



注:Windowsでは、プロセスの除外はエンジンごとに適用されます。同じ除外を複数のエンジンに適用する必要がある場合は、該当する各エンジンに対してプロセス除外を複製する必要があります。

プロセスワイルドカード：

Secure Endpoint Windowsコネクタは、プロセスの除外内でワイルドカードを使用してサポートします。これにより、除外される項目が少なく適用範囲が広くなりますが、定義されていない項目が多すぎる場合は危険です。ワイルドカードは、必要な除外を指定するために必要な最小文字数をカバーするためだけに使用する必要があります。

Windowsのプロセスワイルドカードの使用：

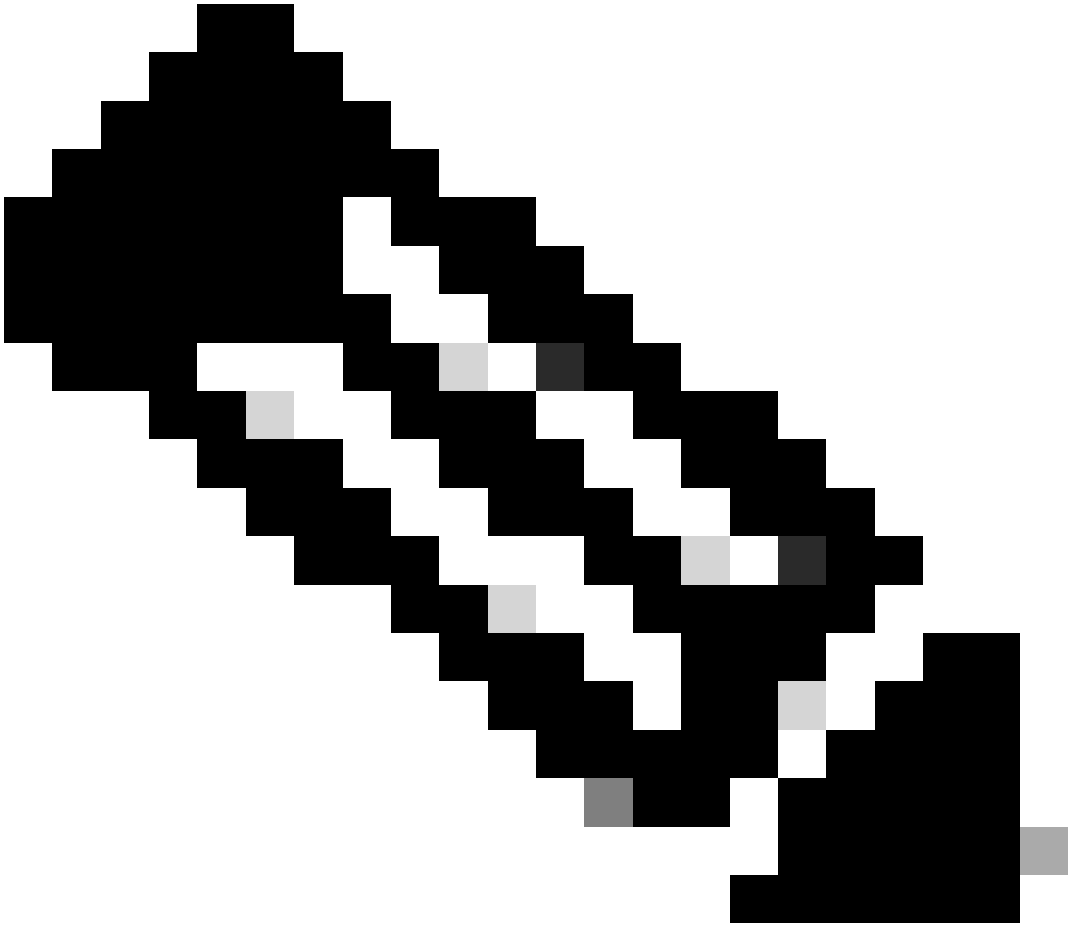
- ワイルドカードは、単一のアスタリスク文字()と二重のアスタリスク(*)を使用して表されます
- アスタリスク(*)を1つ入力：
  - ワイルドカードは、単一文字またはディレクトリ全体の代わりに使用できます。
  - パスの先頭にワイルドカードを配置することは無効と見なされます。
  - ワイルドカードは、スラッシュまたは英数字の2つの定義済み文字の間で機能します。
  - パスの最後にワイルドカードを置くと、そのディレクトリ内のすべてのプロセスが除外されますが、サブディレクトリは除外されません。
- ダブルアスタリスクのワイルドカード(**):
  - パスの終端にのみ配置できます。
  - パスの最後にワイルドカードを置くと、そのディレクトリ内のすべてのプロセスとサブディレクトリ内のすべてのプロセスが除外されます。
  - これにより、最小限の入力で非常に大きな除外セットが可能になりますが、可視性のために非常に大きなセキュリティホールが残ります。この機能は、細心の注意を払って使用してください。

例:

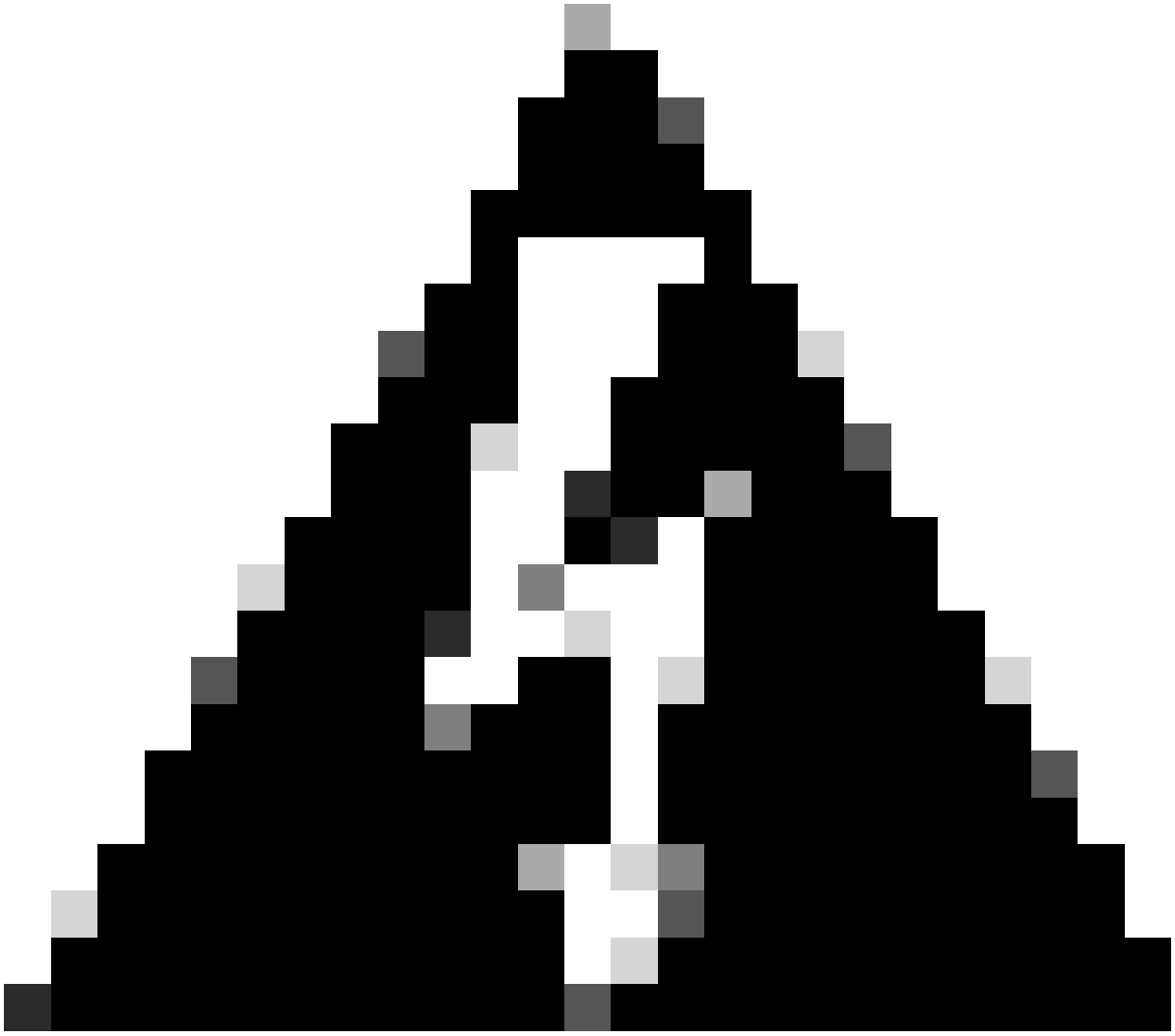
除外	予想される結果
C:\Windows*\Tiworker.exe	Windowsのサブディレクトリにあるすべての Tiworker.exe プロセスを除外します。
C:\Windows\P*t.exe（登録ユーザ専用）	Pot.exe、Pat.exe、P1t.exeなどは除外されます。
C:\Windows*chickens.exe	Windowsディレクトリ内で chickens.exe で終わるすべてのプロセスを除外します。
C:*	C: ドライブ内のすべてのプロセスを除外しますが、サブディレクトリ内のプロセスは除外しません
C:**	C: ドライブ上のすべてのプロセスを除外

脅威の除外

脅威の除外により、特定の脅威名をトリガーイベントから除外できます。脅威の除外は、イベントが誤検出の結果であることが確実な場合にのみ使用する必要があります。この場合、脅威の除外として、イベントからの正確な脅威名を使用します。このタイプの除外を使用する場合、脅威名の検出時に検出時に検出時に検出時に脅威が検出されたり、隔離されたり、イベントが生成されたりすることはありません。



注：脅威の除外では、大文字と小文字は区別されません。例：`W32.Zombies.NotAVirus`とw32.zombies.notavirusはどちらも同じ脅威名に一致しています。



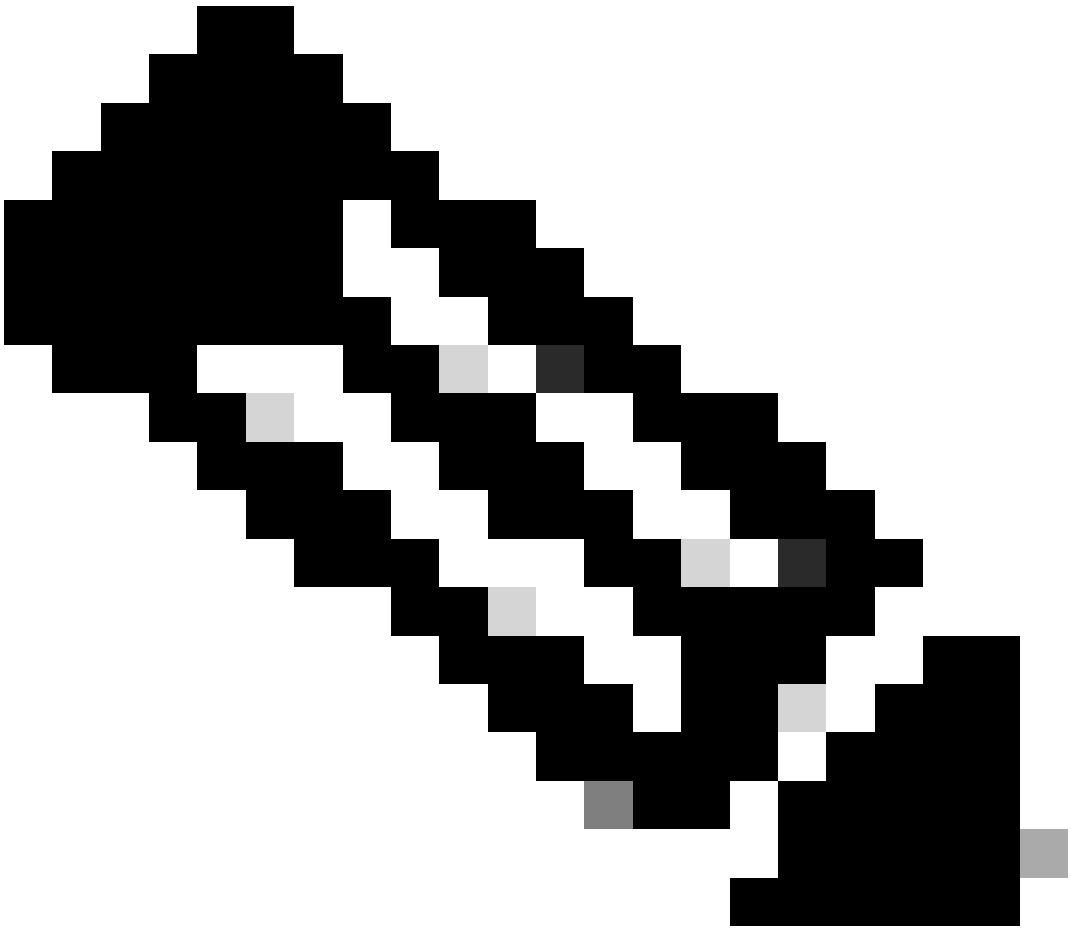
警告：徹底的な調査により脅威名が誤検出されていることが確認された場合を除き、脅威を除外しないでください。除外された脅威は、レビューや監査のためにイベントタブに表示されなくなりました。

パスの除外

アプリケーションの競合は通常、ディレクトリの除外を伴うため、パスの除外が最も頻繁に使用されます。絶対パスを使用してパス除外を作成できます。Windowsでは、CSIDILまたはKNOWNFOLDERIDを使用してパスの除外を作成することもできます。

たとえば、Windowsの`Program Files`ディレクトリ内のAVアプリケーションを除外する場合、除外パスは次のいずれかになります。

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



注：パスの除外は再帰的であり、すべてのサブディレクトリも除外します。

部分的なパスの一致（Windowsのみ）

パスの除外に末尾のスラッシュが指定されていない場合、Windowsコネクタはパスの部分一致を行います。MacとLinuxでは、パスの部分的な一致はサポートされていません。

たとえば、Windowsで次のパスの除外を適用する場合は、

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

その後、次のパスはすべて除外されます。

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

「C:\test」からの除外を「C:\test\」に変更すると、「C:\test123」が除外されなくなります。

ファイル拡張子の除外

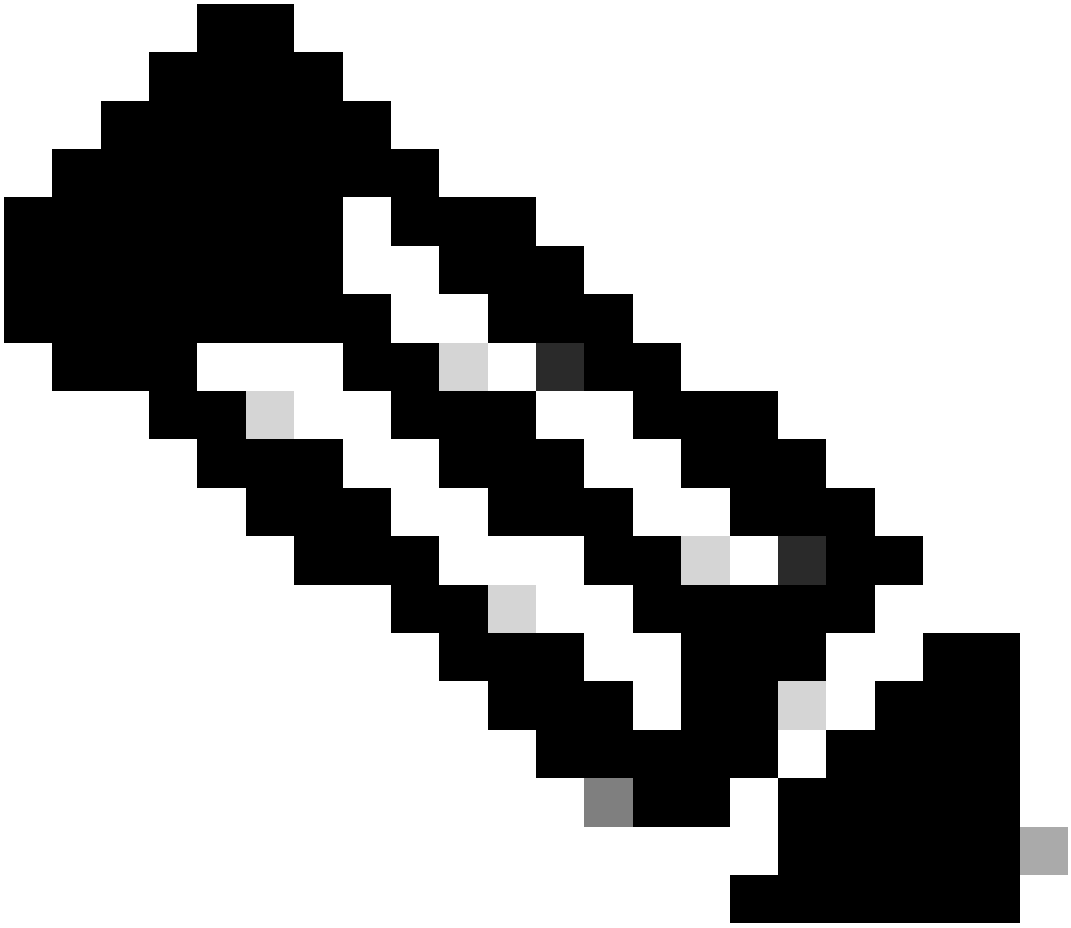
ファイル拡張子の除外では、特定の拡張子を持つすべてのファイルを除外できます。

キー ポイント：

- セキュアエンドポイントコンソールで必要な入力は.extensionです。
- ファイル拡張子が追加されていない場合は、Secure Endpoint Consoleによって自動的にファイル拡張子の先頭にピリオドが追加されます。
- 拡張子は大文字と小文字を区別しません。

たとえば、すべてのMicrosoft Accessデータベースファイルを除外するには、次の除外を作成します。

.MDB



注：標準のファイル拡張子による除外は、デフォルトのリストで使用できます。これらの除外を削除することはお勧めできません。削除すると、エンドポイントのパフォーマンスが変更される可能性があります。

ワイルドカードの除外

ワイルドカードの除外は、パスまたはファイル拡張子の除外と同じですが、パスまたは拡張子の中でワイルドカードを表すためにアスタリスク(*)を使用できる点が異なります。

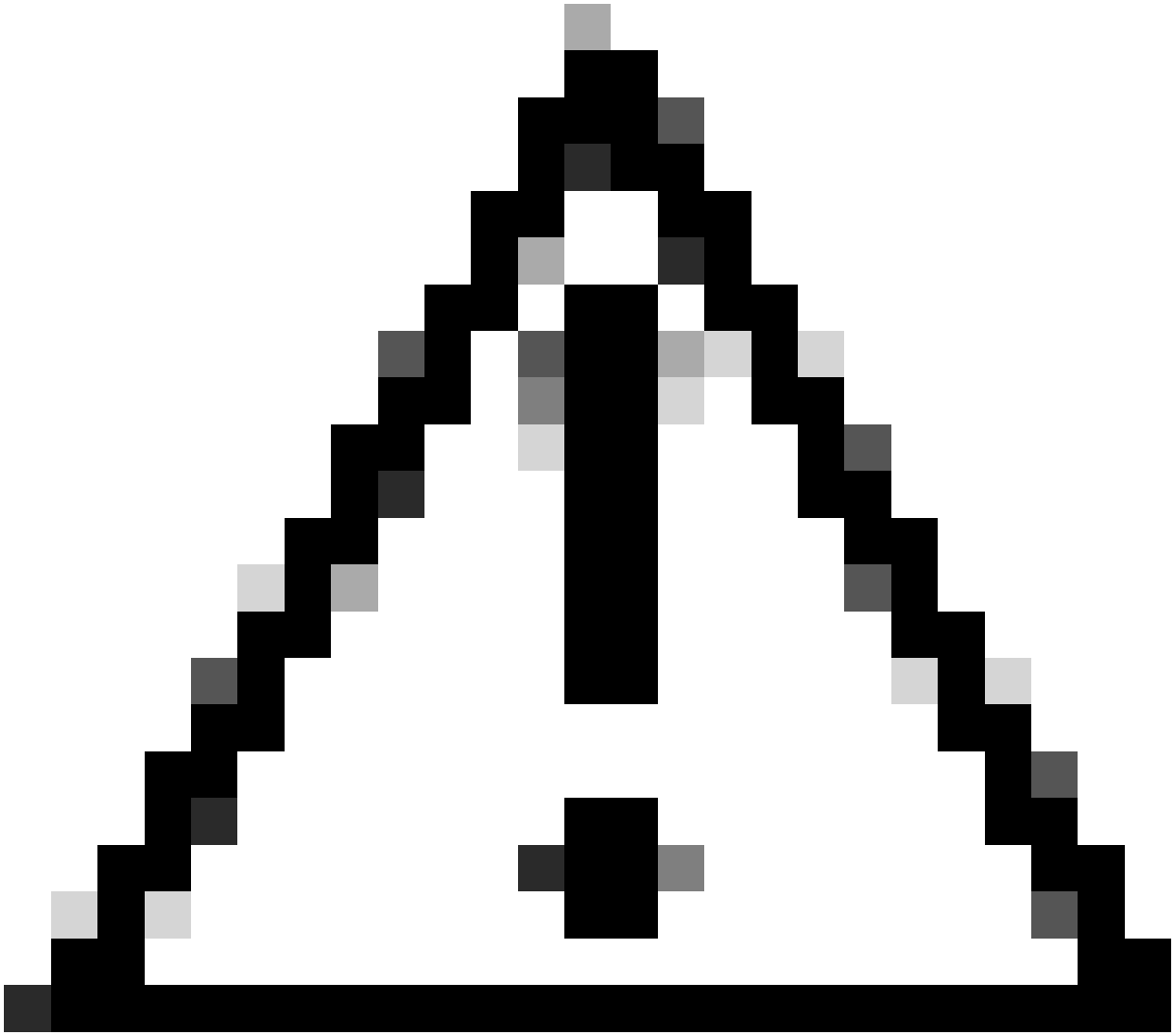
たとえば、macOS上の仮想マシンをスキャンから除外する場合は、次のパス除外を入力します。

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

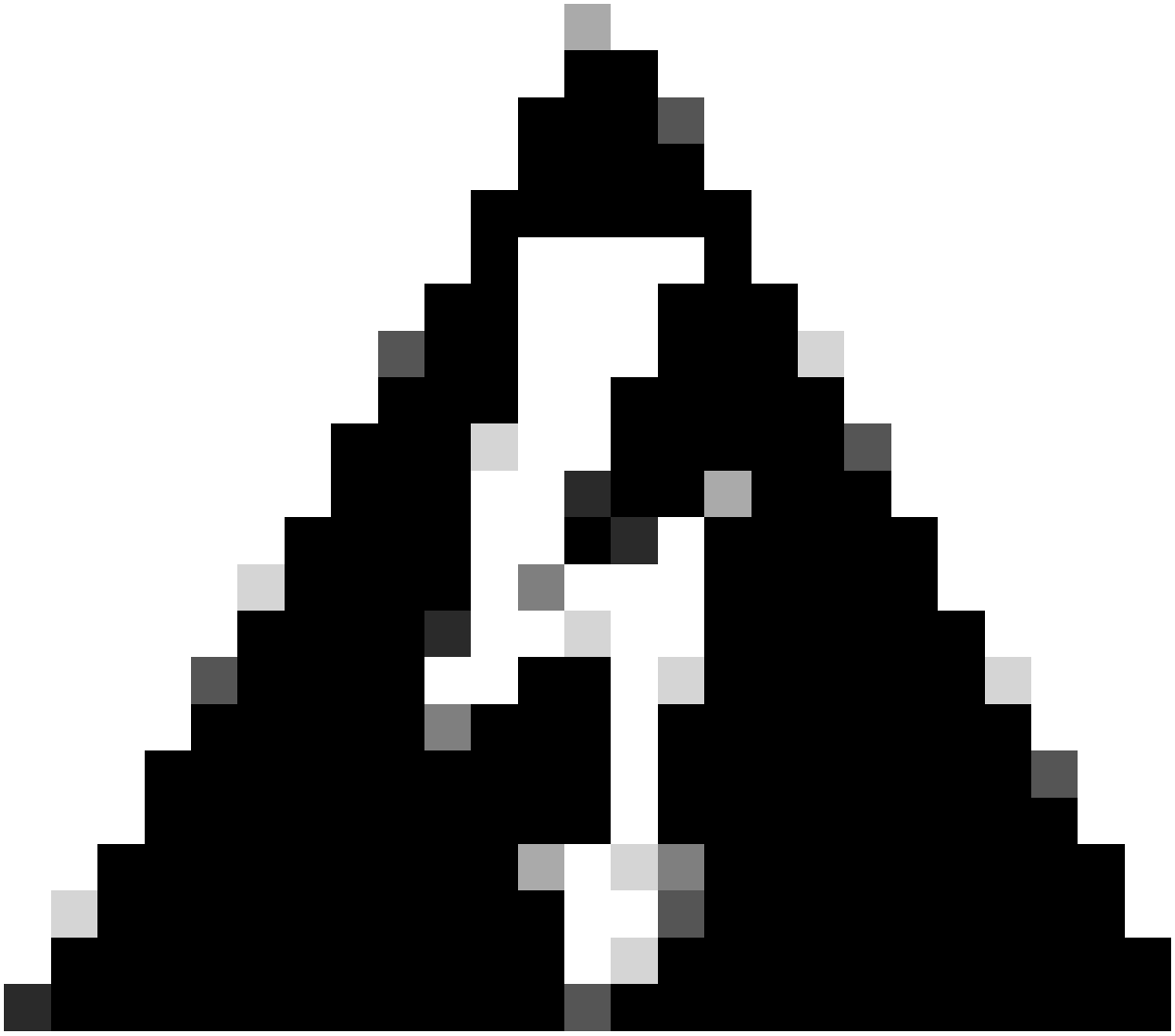
ただし、この除外は1人のユーザに対してのみ機能します。パス内のユーザ名をアスタリスクに置

き換え、ワイルドカード除外を作成して、このディレクトリをすべてのユーザから除外します。

/Users/*/Documents/Virtual Machines/



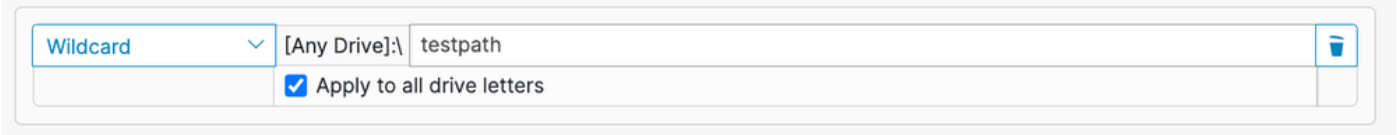
注意：ワイルドカードの除外は、パスの区切り記号で止まることはありません。このため、意図しない除外が行われる可能性があります。たとえば、C:*\test は C:\sample\testとC:\1\test** またはC:\sample\test123を除外します。



警告：アスタリスクで除外を開始すると、パフォーマンスに重大な問題が発生する可能性があります。CPUへの影響を軽減するには、アスタリスク(*)で始まるすべての除外を削除または変更します。

Windows

Windowsでワイルドカード除外を作成する場合、すべてのドライブ文字に適用するオプションがあります。このオプションを選択すると、ワイルドカードの除外がすべてのマウントされたドライブに適用されます。



同じ除外を手動で作成する場合は、^[A-Za-z]を先頭に付加する必要があります。次に例を示します。

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

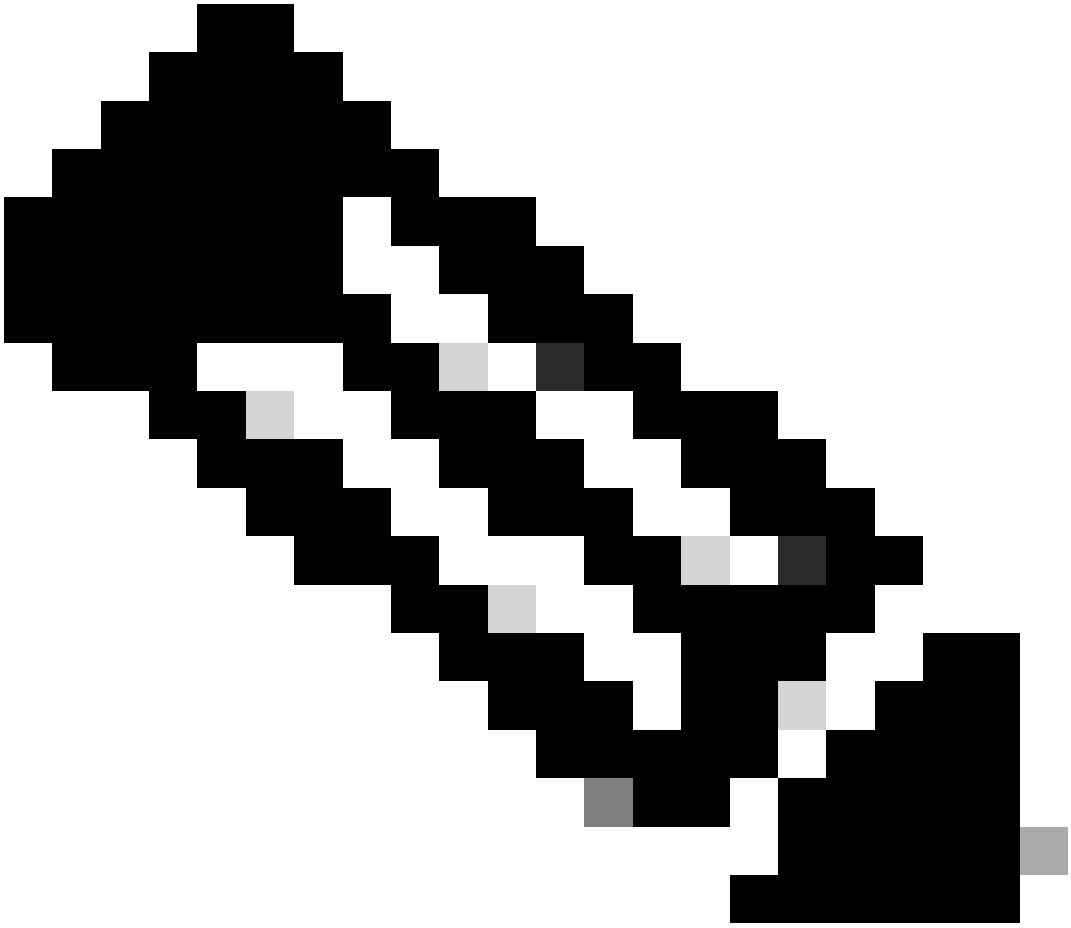
どちらの例でも、C:\testpathおよびD:\testpathは除外されます。

ワイルドカード除外に対して`Apply to all drive letters`が選択されている場合、Secure Endpoint Consoleは自動的に`^[A-Za-z]`を生成します。

実行可能ファイルの除外（Windowsのみ）

実行可能ファイルの除外は、エクスプロイト防止が有効になっているWindowsコネクタにのみ適用されます。実行可能ファイルを除外すると、特定の実行可能ファイルが不正利用の防止によって保護されなくなります。問題やパフォーマンスの問題が発生している場合にだけ、実行可能ファイルを不正利用の防止から除外する必要があります。

保護されたプロセスの一覧を確認し、アプリケーションの除外フィールドに実行可能ファイル名を指定して、保護から除外することができます。実行可能ファイルの除外は、`name.exe`形式の実行可能ファイル名と正確に一致する必要があります。ワイルドカードはサポートされていません。

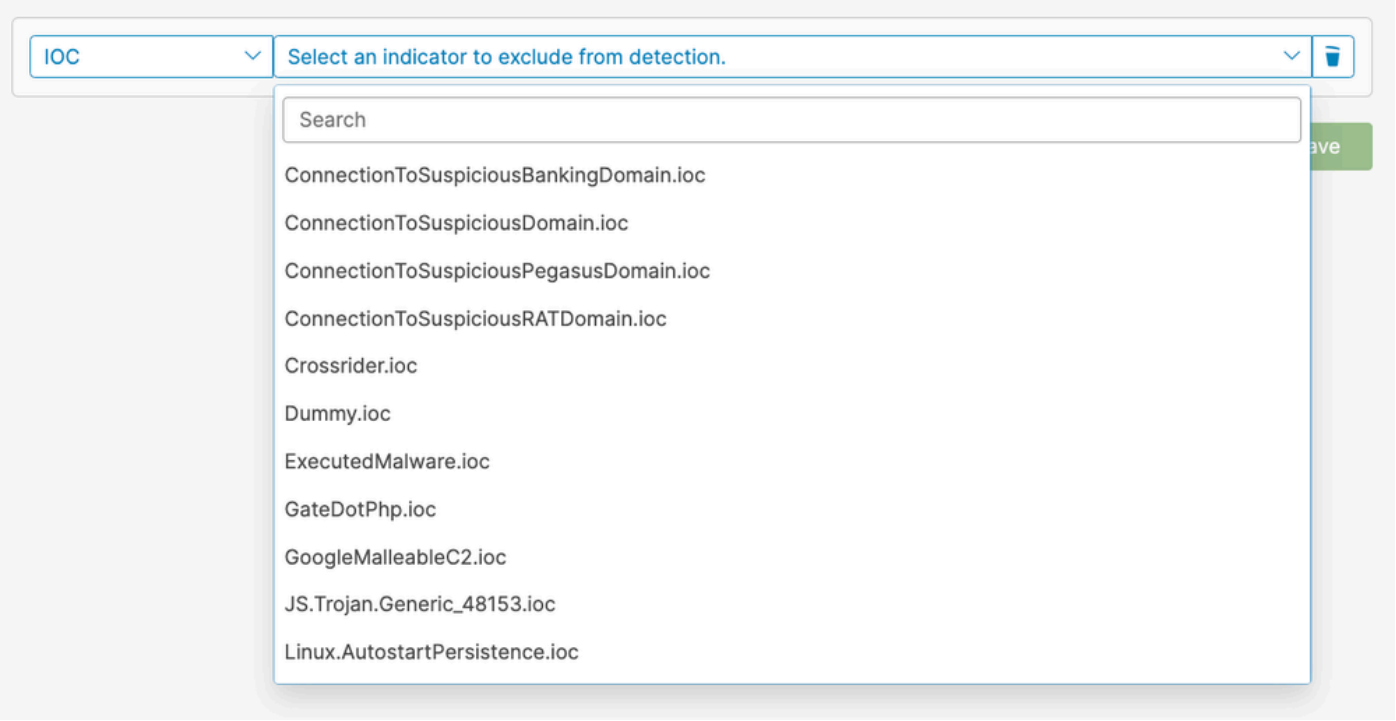


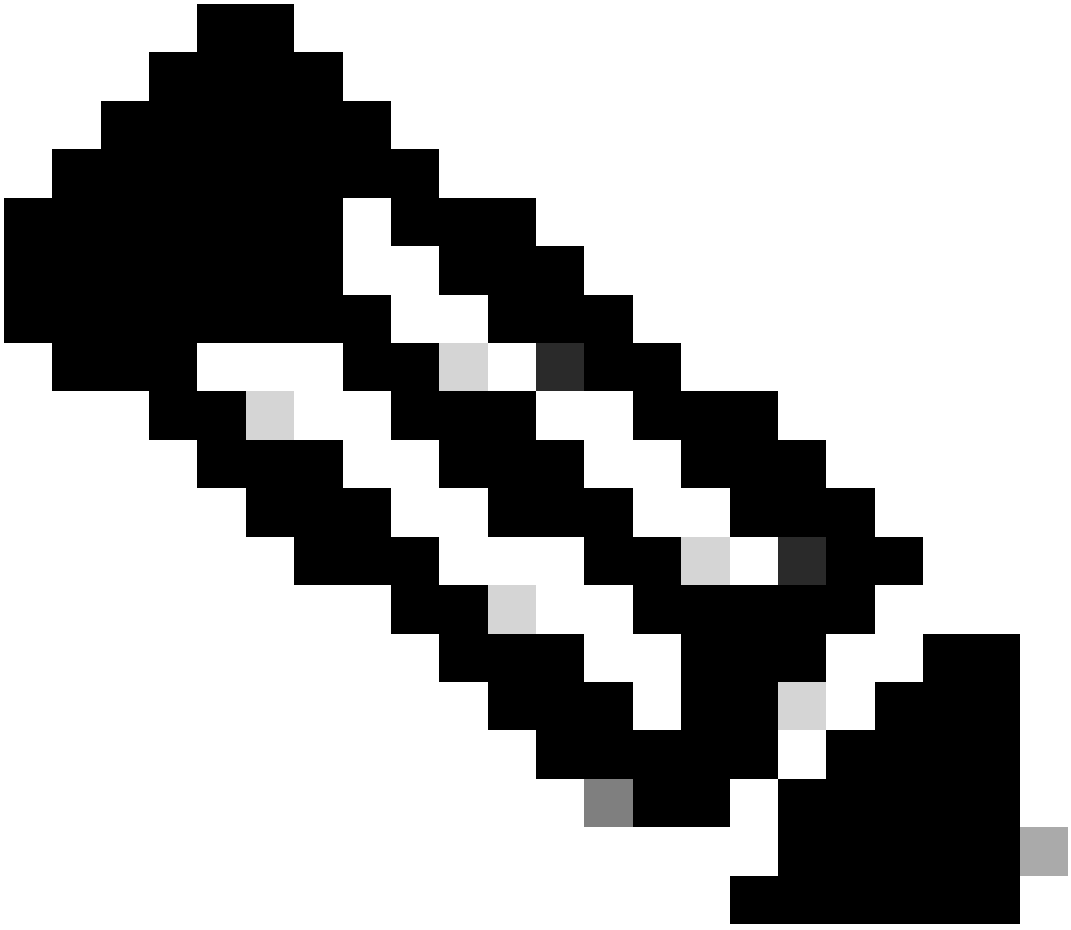
注:Secure Endpoint Consoleで実行可能ファイルの除外を使用して除外できるのは、アプリケーションだけです。DLLに関連する除外を作成するには、サポートケースを開く必要があります。

エクスプロイト防止の正しい除外を見つけるには、他の除外タイプよりもはるかに集中的なプロセスが必要です。また、セキュリティホールを最小限に抑えるために広範なテストが必要です。

IOCの除外（Windowsのみ）

IOCの除外により、クラウドの侵入の痕跡を除外できます。これは、署名されていない可能性があり、特定のIOCを頻繁にトリガーする原因となるカスタムアプリケーションまたは内部アプリケーションがある場合に便利です。Secure Endpoint Consoleには、IOCの除外に関するインジケータのリストが表示されます。除外するインジケータをドロップダウンから選択できます。


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



注：重大度が高いまたは重大なIOCを除外すると、IOCへの可視性が失われ、組織がリスクにさらされる可能性があります。これらのIOCが誤検出される回数が多い場合にのみ、除外する必要があります。

CSIDLおよびKNOWNFOLDERID（Windowsのみ）

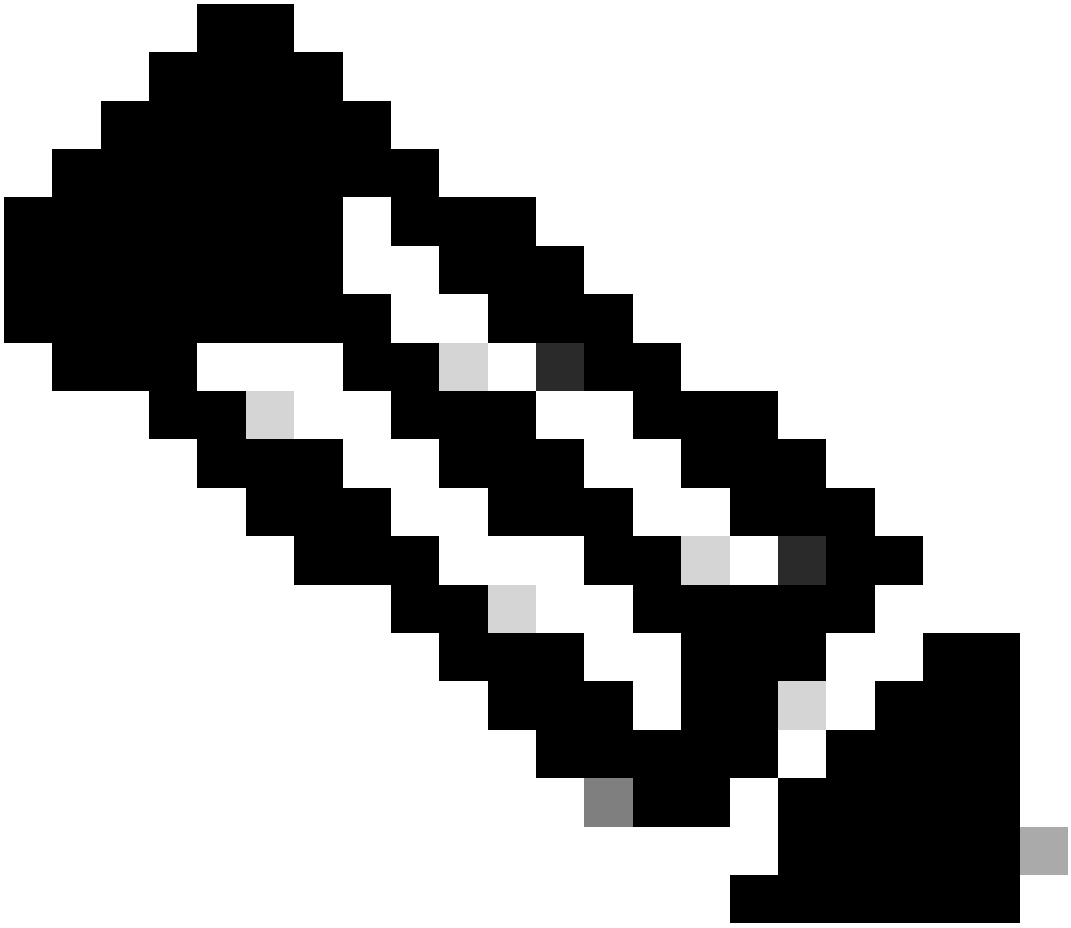
Windowsのパスとプロセスの除外を記述する場合は、CSIDLとKNOWNFOLDERIDの値を受け入れ、推奨します。CSIDL/KNOWNFOLDERID値は、代替ドライブ文字を使用する環境のプロセスとパスの除外を作成する場合に便利です。

CSIDL/KNOWNFOLDERIDを使用する場合は、考慮する必要のある制限があります。環境で複数のドライブ文字にプログラムをインストールする場合、CSIDL/KNOWNFOLDERIDの値は、既定または既知のインストール場所としてマークされているドライブのみを参照します。

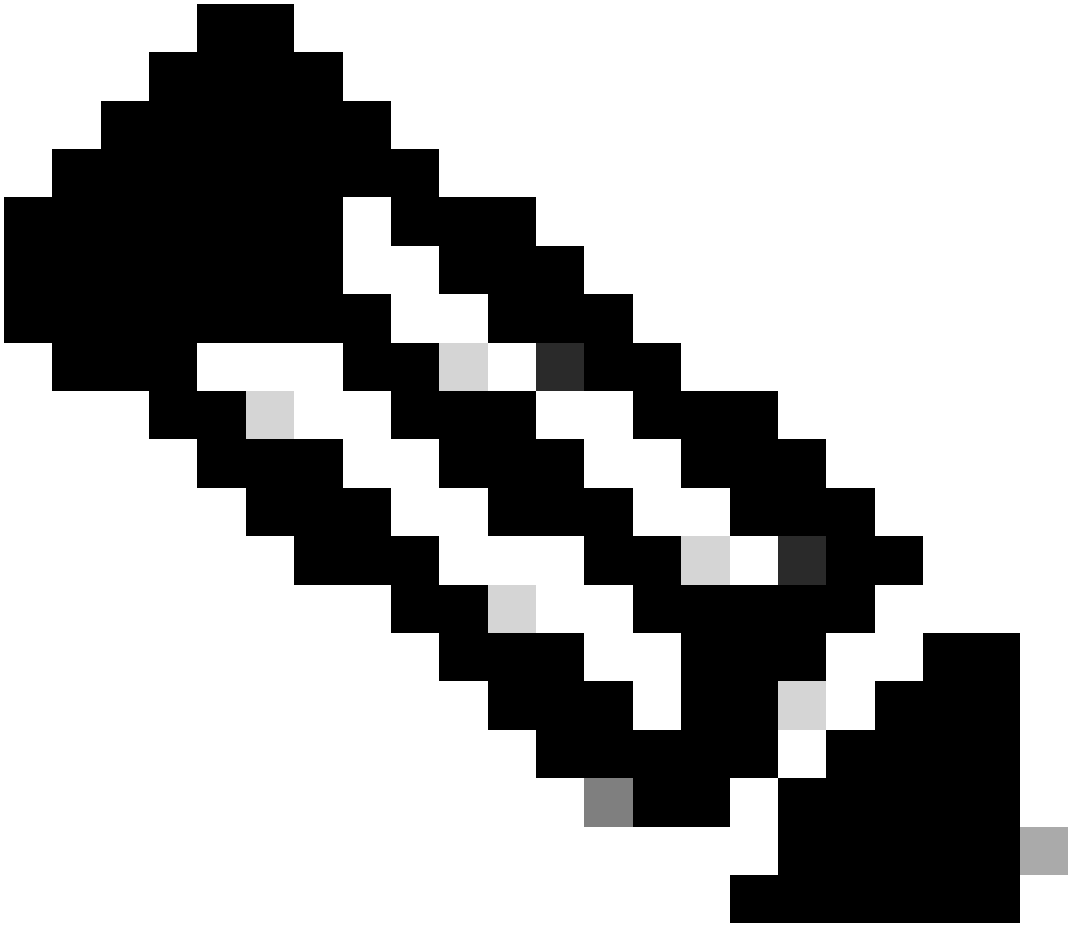
たとえば、OSが`C:\`にインストールされていても、Microsoft SQLのインストールパスが手動で`D:\`に変更されている場合、維持対象除外リストでのCSIDL/KNOWNFOLDERIDベースの除外は、そのパスには適用されません。つまり、CSIDL/KNOWNFOLDERIDを使用するとマップされないため、`C:\`ドライブにないパスまたはプロセスの除外ごとに1つずつ除外を入力する必要があります。

詳細については、次のWindowsのマニュアルを参照してください。

- CSIDL
- KNOWNFOLDERID



注: KNOWNFOLDERIDは、Windowsコネクタ8.1.7以降でのみサポートされています。以前のバージョンのWindowsコネクタでは、CSIDL値を使用します。



注意: KNOWNFOLDERID値では、大文字と小文字が区別されます。たとえば、無効な `valueFolderID_programfiles`ではなく`valueFOLDERID_ProgramFiles`を使用する必要があります。

除外チューニング用のコネクタの準備

除外チューニング用にコネクタを準備するには、次の操作を行う必要があります。

1. デバッグモードで実行するポリシーとグループを設定します。
2. 通常の業務に従って新しいデバッググループのコンピュータを実行し、十分なコネクタログデータを取得する時間を確保します。
3. 除外の識別に使用するコネクタの診断データを生成します。

デバッグモードを有効にし、異なるオペレーティングシステムで診断データを収集する手順については、次の文書を参照してください。

- Cisco Secure Endpoint Connector for Mac診断データ収集

- Linux診断データ収集用Cisco Secure Endpoint Connector
- 高CPU用AMP診断バンドルの分析(Windows)

除外の特定

MacOSおよびLinux

デバッグモードで生成された診断データには、除外の作成に役立つ2つのファイルfileops.txtとexecs.txtが用意されています。fileops.txtファイルはパス/ファイル拡張子/ワイルドカード除外の作成に役立ち、execs.txtファイルはプロセス除外の作成に役立ちます。

プロセスの除外の作成

execs.txtファイルには、セキュアエンドポイントがファイルスキャンを実行するトリガーとなった実行可能パスがリストされています。各パスには、スキャンの回数を示すカウントが関連付けられ、リストは降順にソートされます。このリストを使用して、大量の実行イベントが発生しているプロセスを特定し、プロセスパスを使用して除外を作成できます。ただし、一般的なユーティリティプログラム（/usr/bin/grepなど）やインタプリタ（/usr/bin/rubyなど）を除外することは推奨されません。一般的なユーティリティプログラムやインタープリタが大量のファイルスキャンを生成している場合は、さらに調査を行って、対象を絞った除外を試みることができます。

1. 親プロセスの除外：プロセスを実行しているアプリケーションを特定し（たとえば、grepを実行している親プロセスを見つけます）、この親プロセスを除外します。これは、親プロセスがプロセスの除外に安全に設定できる場合にのみ行う必要があります。親プロセスの除外が子プロセスに適用される場合、親プロセスからの子プロセスの呼び出しも除外されます。
2. 特定のユーザーのプロセスを除外する：プロセスを実行しているユーザーを特定します。特定のユーザーによって大量にプロセスが実行されている場合は、その特定のユーザーのプロセスだけを除外できます（たとえば、ユーザー「root」によってプロセスが大量に呼び出されている場合は、そのプロセスを除外できますが、指定したユーザー「root」に対してのみ除外できます。これにより、Secure Endpointは、「root」以外のユーザーによる特定のプロセスの実行を監視できます）。

execs.txtの出力例を次に示します。

```
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
```

パス、ファイル拡張子、およびワイルドカードの除外の作成

fileops.txtファイルには、ファイルの作成、変更、名前変更のアクティビティによってSecure Endpointがファイルスキャンを実行するトリガーとなったパスがリストされています。各パスには、スキャンの回数を示すカウントが関連付けられ、リストは降順にソートされます。パスの除外を開始する1つの方法は、fileops.txtから最も頻繁にスキャンされるファイルおよびフォルダパスを見つけ、それらのパスのルールを作成することを検討することです。カウントが高いからといって、必ずしもパスを除外する必要があるわけではありませんが（たとえば、電子メールを保存するディレクトリを頻繁にスキャンできますが、除外する必要はありません）、除外の候補を特定するための開始点となります。

fileops.txtの出力例：

```
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
```

経験則として、ログファイルまたはジャーナルファイルの拡張子を持つものは、すべて適切な除外候補と見なす必要があります。

動作保護エンジン

動作保護エンジンは、Linuxコネクタバージョン1.22.0とmacOSコネクタバージョン1.24.0で導入されました。これらのバージョン以降、このコネクタは圧倒的に高いシステムアクティビティを検出し、障害18を引き起こします。

プロセスの除外はすべてのエンジンとファイルスキャンに適用されます。この障害を修復するには、プロセスの除外を非常にアクティブな良性プロセスに適用します。デバッグモード診断データによって生成されたtop.txtファイルを使用して、システム上で最もアクティブなプロセスを特

定できます。詳細な修復手順については、『セキュアエンドポイントMac/Linuxコネクタ障害18』のガイダンスを参照してください。

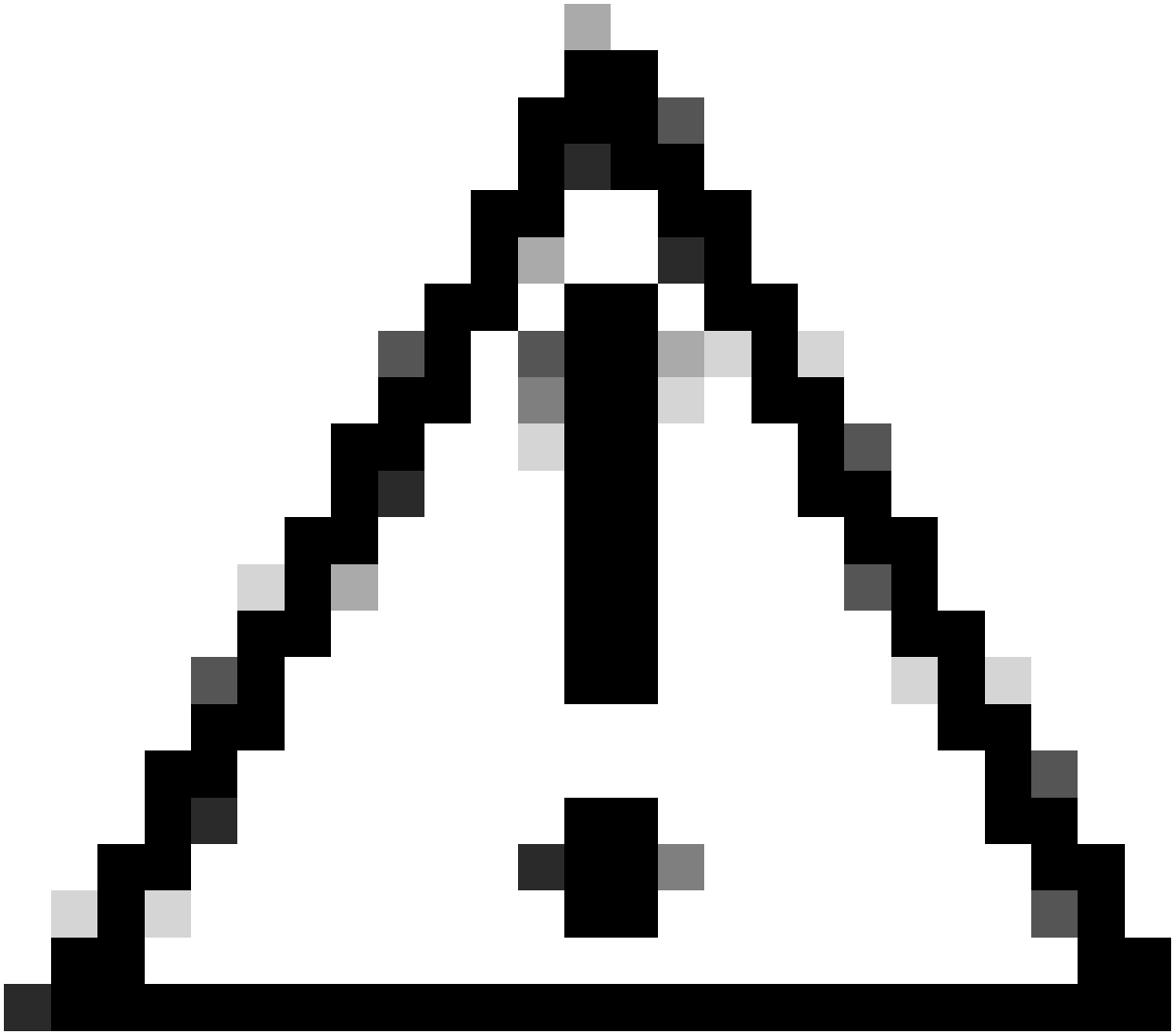
さらに、プロセスの除外により、良性ソフトウェアからの誤検出の動作保護を抑制できます。Secure Endpoint Consoleで誤検出が発生した場合は、このプロセスを除外してレポートを向上させることができます。

Windows

Windowsオペレーティングシステムはより複雑で、親プロセスと子プロセスのために、より多くの除外オプションが利用可能です。これは、アクセスされたファイルだけでなく、それらを生成したプログラムを特定するために、より深いレビューが必要であることを示しています。

セキュアエンドポイントを使用してWindowsのパフォーマンスを分析し、最適化する方法の詳細については、Cisco SecurityのGitHubページにあるWindowsチューニングツールを参照してください。

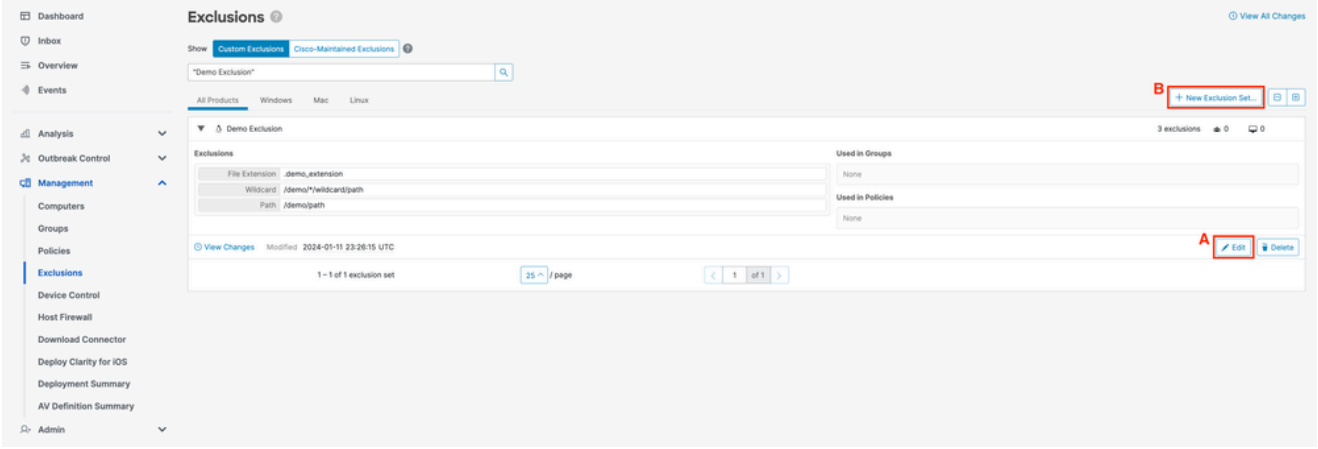
セキュアエンドポイントコンソールでの除外ルールの作成



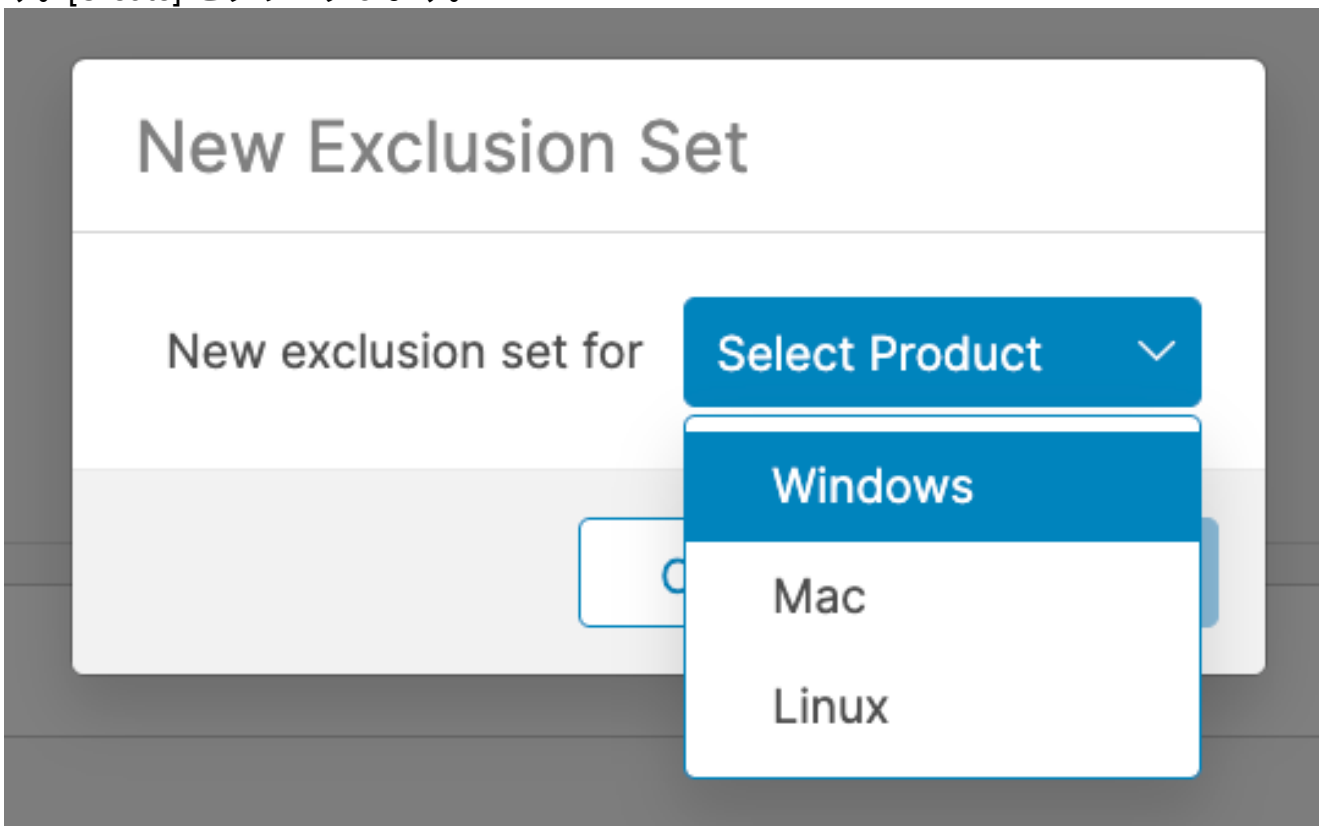
注意：除外を書き込む前に、必ずファイルとプロセスを理解して、エンドポイントのセキュリティ脆弱性を回避してください。

セキュアエンドポイントコンソールを使用して新しい除外ルールを作成するには、次の手順を実行します。

1. Secure Endpoint Consoleで、`Management` -> `Exclusions`の順に選択して、Policiesページに移動します。(A)変更する除外セットを見つけて、`Edit`をクリックするか、(B)+ New Exclusion Set...をクリックします。

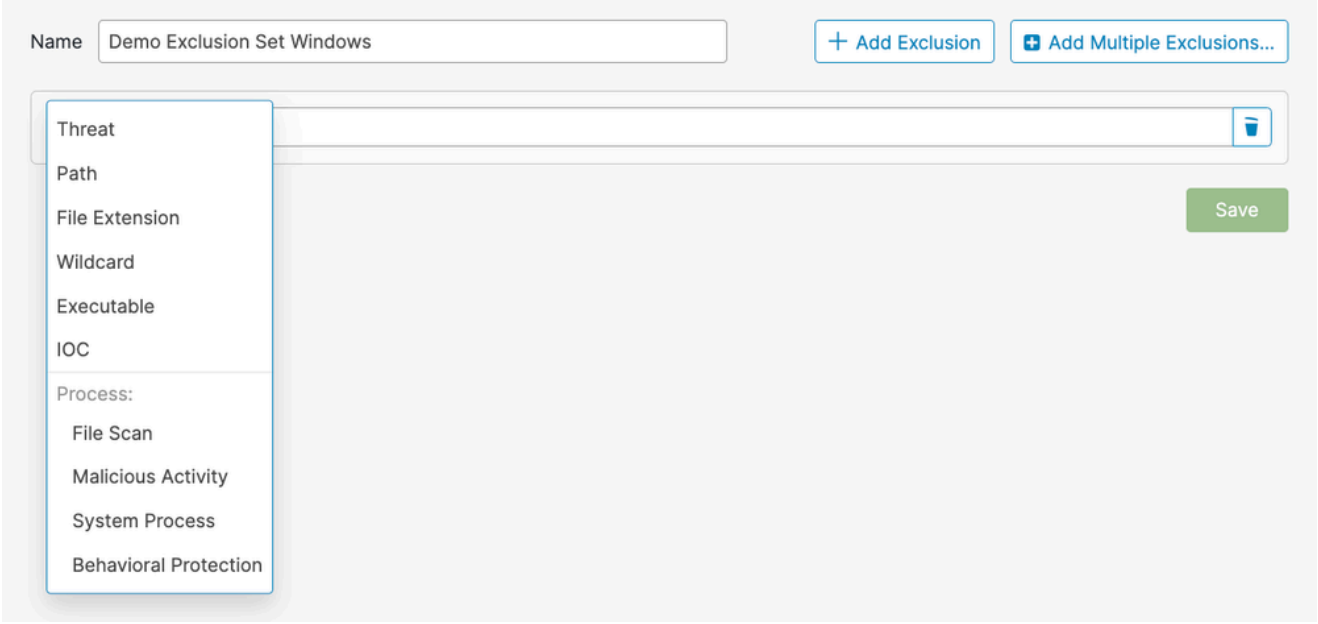


2. 新しい除外セットポップアップで、除外セットを作成するオペレーティングシステムを選択します。[Create] をクリックします。

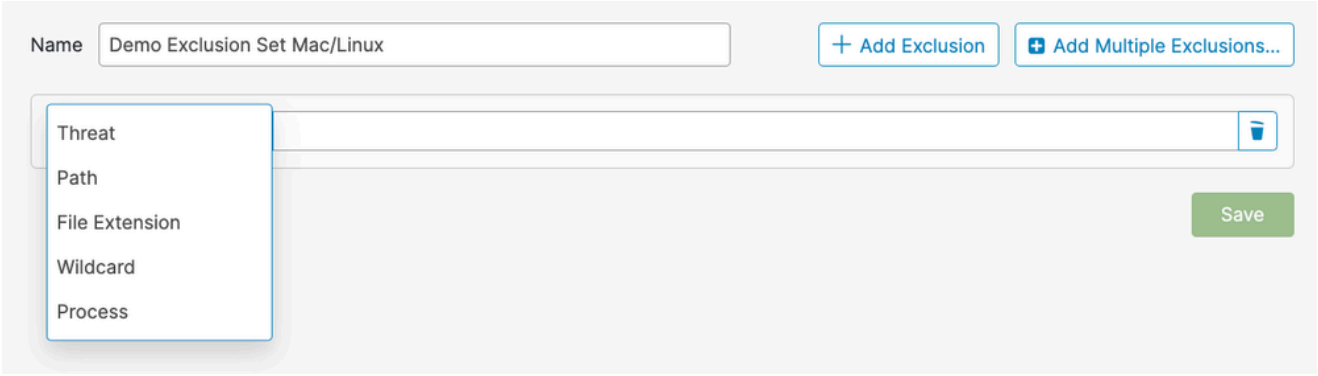


3. 新しい除外セットのページにリダイレクトされます。+除外の追加をクリックして、タイプの選択ドロップダウンから除外タイプを選択します。

Windows：



Mac/Linux:



4. 選択した除外タイプの必須フィールドに入力します。
5. さらにルールを追加するには、ステップ2と3を繰り返します。除外セットを保存するには、Saveをクリックします。

ベスト プラクティス

除外を作成すると、Cisco Secure Endpointによって提供される保護レベルが低下するため、注意が必要です。除外されたファイルは、キャッシュまたはクラウドでハッシュ、スキャン、または利用可能ではなく、アクティビティは監視されず、バックエンドエンジン、デバイストラジェクトリー、および高度な分析から情報が欠落します。

除外は、特定のアプリケーションとの互換性の問題や、他の方法では改善できないパフォーマンスの問題など、対象を絞ったインスタンスでのみ使用する必要があります。

除外を作成する際に従うべきベストプラクティスは次のとおりです。

- 実証済みの問題に対してのみ除外を作成
  - 他の方法では対処できない問題であることが証明されていない限り、除外が必要であると仮定しないでください。
  - 除外を適用する前に、パフォーマンスの問題、誤検出、またはアプリケーションの互換性の問題を徹底的に調査し、軽減する必要があります。
- パス/ファイル拡張子/ワイルドカードの除外よりもプロセスの除外を優先

    - プロセスの除外では、パス、ファイル拡張子、およびワイルドカードの除外を組み合わせて同じ結果を得るよりも、良性ソフトウェアのアクティビティを直接除外できます。
    - 可能な場合は、プログラム実行可能ファイルを対象とするパス、ファイル拡張子、およびワイルドカードの除外を、対応するプロセスの除外に置き換えることをお勧めします。
- 広範な除外の回避
    - Cドライブ全体など、エンドポイントの大部分を除外しないでください。
    - ファイル名だけでなく、ファイルへの完全修飾パスを使用します。
    - デバイストラジェクトリー、Secure Endpoint Diagnostics Data、およびWindowsチューニングツールを使用して、特定の除外を調査して決定します。
- ワイルドカードの除外を過剰に使用しない
    - ワイルドカードを使用して除外を作成する場合は注意してください。可能な場合は、より具体的な除外を使用します。
    - ワイルドカードの最小数を除外に使用します。ワイルドカードを使用できるのは、真に可変なフォルダのみです。
- 一般的なユーティリティプログラムやインタプリタを除外しないでください
    - 一般的なユーティリティプログラムやインタープリタを除外することは推奨されません。
    - 一般的なユーティリティプログラムやインタプリタを除外する必要がある場合は、プロセスユーザを指定します（macOS/Linuxのみ）。
    - たとえば、python、`java`、`ruby`、`bash`、`sh`などの例外を書くことは避けてください。
- 重複した除外の回避
    - 除外を作成する前に、カスタム除外またはCisco-Maintained除外のいずれかに除外がすでに存在するかどうかを確認します。
    - 重複する除外を削除すると、パフォーマンスが向上し、除外の運用管理が軽減されます。
    - プロセスの除外で指定されたパスが、パス/ファイル拡張子/ワイルドカードの除外の対象となっていないことを確認してください。
- マルウェア攻撃でよく使用されるプロセスを除外しない
    - 詳細は、『推奨されない除外』を参照してください。
- 古い除外の削除
    - 除外リストを定期的に確認して監査し、特定の除外が追加された理由を記録します。
- セキュリティ侵害の除外の削除
    - 最適なセキュリティと可視性を取り戻すには、除外を解除してコネクタを侵害する必要があります。
    - 自動化されたアクションを使用して、感染後にコネクタにより安全なポリシーを適用できます。コネクタが侵害された場合、最高レベルの保護が確実に適用されるように、除外されていないポリシーを含むグループにコネクタを移動する必要があります。
    - 「Move Computer to Group Upon Compromise」自動処理を事前に設定する方法の詳細については、「Identify Conditions to Trigger Automated Actions in Secure Endpoint」を参照してください。
- 除外するアイテムの保護を強化する
    - 除外が絶対に必要な場合は、書き込み保護を有効にして除外する項目の保護レイヤを追加するなど、緩和策を検討してください。
- 除外をインテリジェントに作成

    - ルールを最適化するには、除外するアプリケーションを一意に識別する最上位レベルの親プロセスを選択し、「子プロセスに適用」オプションを使用してルールの数を最小限にします。
- 起動プロセスを除外しない
    - 起動プロセス(macOSでは`launchd`、Linuxでは`init`または`systemd`)は、システム上の他のすべてのプロセスを起動する役割を担い、プロセス階層の最上位にあります。
    - 起動プロセスとそのすべての子プロセスを除外すると、セキュアエンドポイントのモニタリングが実質的に無効になります。
- 可能な場合は、プロセスユーザを指定します（macOS/Linuxのみ）。
    - [ユーザー]フィールドを空白のままにすると、指定したプログラムを実行しているすべてのプロセスに除外が適用されます。
    - 任意のユーザに適用される除外はより柔軟ですが、この広範なスコープは、意図せずに監視する必要があるアクティビティを除外する可能性があります。
    - ランタイムエンジン(`java`など)やスクリプトインタープリタ(`bash`、`python`など)などの共有プログラムに適用されるルールでは、ユーザの指定が特に重要です。
    - ユーザを指定すると、スコープが制限され、Secure Endpointが他のインスタンスを監視しながら特定のインスタンスを無視するように指示されます。

推奨されない除外

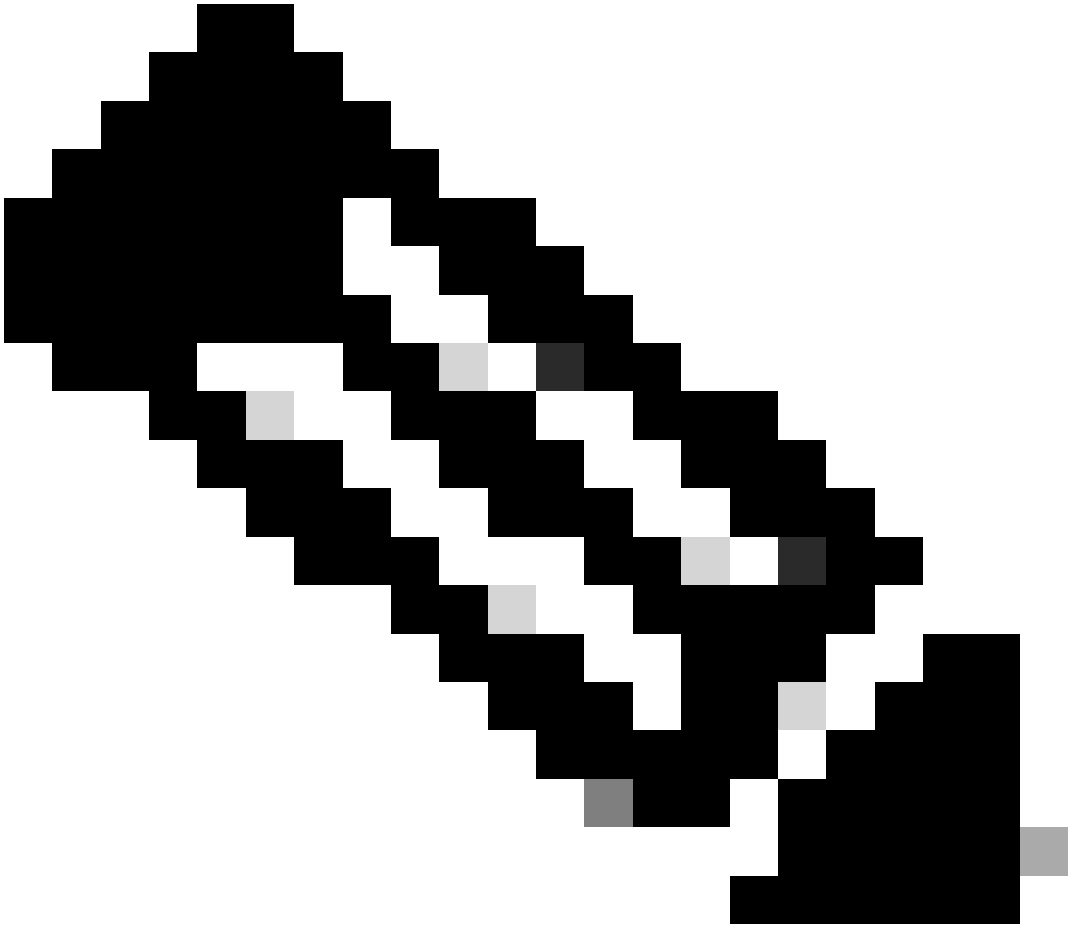
攻撃者が使用する可能性のあるすべての攻撃ベクトルを知ることは不可能ですが、監視する必要があるコア攻撃ベクトルがいくつかあります。良好なセキュリティポスチャと可視性を維持するために、次の除外は推奨されません。

AcroRd32.exe（入手可能）
addinprocess.exe
addinprocess32.exe（入手可能）
addinutil.exe
bash.exe (bash.exe)
bginfo.exe（入手可能）
bitsadmin.exe
cdb.exe（入手可能）
csi.exeファイル
dbghost.exe
dbgsvc.exe
dnx.exe
dotnet.exe
excel.exe（ダウンロード）
fsi.exe（入手可能）
fsiAnyCpu.exe（入手可能）
iexplore.exe
java.exe（ダウンロード）
kd.exe
lxssmanager.dll

msbuild.exe（ビルドのセットアップ）
mshta.exe
ntkd.exe
ntsd.exe
outlook.exe
psexec.exe
powerpnt.exe（登録ユーザ専用）
powershell.exe
rcsi.exe
svchost.exe
schtasks.exe
system.management.automation.dll（自動）
windbg.exe（ベータ版）
winword.exe
wmic.exe（登録ユーザ専用）
wuauclt.exe
0.7z
.bat
.bin
.cab
.cmd（コマンドラインインターフェイス）
.com
.cpl
.dll
.exe
.fla
.gif
.gz
.hta
.inf
.java
.jar
ジョブ
.jpeg
.jpg
.js
.ko
.ko.gz
.msi
.ocx
.png
.ps1

.py
.rar
.reg
.scr
.sys
.tar
.tmp
.url
.vbe
.vbs
.wsf
.zip
バッシュ
java
Pythonの
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 Files\<会社名>\

C:\Programファイル(x86)\<会社名>\
C:\Users\<UserProfileName>\AppData\Local\Temp\
C:\Users\<UserProfileName>\AppData\LocalLow\Temp\



注：これは除外すべき項目の完全なリストではありませんが、コア攻撃ベクトルに関する情報を提供します。これらのパス、ファイル拡張子、およびプロセスの可視性を維持することが重要です。

関連情報

- テクニカル サポートとドキュメント - Cisco Systems
- Cisco Secure Endpoint – テクニカルノート
- Cisco Secure Endpoint – ユーザガイド
- セキュアエンドポイントにおける不正利用の防止のトラブルシューティング
- セキュアエンドポイントで自動アクションをトリガーする条件の特定

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。