Uitsluitingen van Cisco Secure Endpoint configureren en identificeren

Inhoud

Inleiding

Dit document beschrijft de beste praktijken om uitsluitingen op het beveiligde endpoint te vinden en te maken.

Bijgedragen door Cisco-engineers.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Toegang tot de Secure Endpoint-console
- Account met beheerdersrechten

- Een praktische kennis van de omgeving van de klant.

Gebruikte componenten

De informatie in dit document is gebaseerd op Windows, Linux en MacOS besturingssystemen.

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

Achtergrondinformatie

Hoe u uitsluitingen te begrijpen

Een uitsluitingsset is een lijst met directory's, bestandsextensies of bedreigingsnamen waarvan u niet wilt dat de Secure Endpoint Connector scant of veroordeelt. Uitsluitingen zijn noodzakelijk om een balans tussen prestaties en beveiliging op een machine te garanderen wanneer endpointbescherming zoals Secure Endpoint is ingeschakeld. Dit artikel beschrijft uitsluitingen voor Secure Endpoint Cloud, TETRA, SPP en MAP.

Ieder milieu is uniek, evenals de entiteit die het controleert, variërend van strikt tot open beleid, waarbij het laatste als een honeypot zou worden geclassificeerd. Aangezien dergelijke uitsluitingen worden gedefinieerd, moeten zij op elke situatie worden toegesneden.

Verschillende uitsluitingen kunnen op twee manieren worden gecategoriseerd, **voor de hand liggende uitsluitingen** en **onbepaalde uitsluitingen**.

Duidelijke uitzonderingen

De duidelijke Uitsluitingen zijn uitsluitingen die gebaseerd op onderzoek en test voor algemeen gebruikte werkende systemen, programma's, en andere veiligheidssoftware zijn tot stand gebracht. Deze uitsluitingen kunt u vinden op de door Cisco bijgehouden uitsluitingslijst in uw console.

> **Opmerking**: aanbevolen wordt om contact op te nemen met andere leveranciers van antivirussoftware (AV) en te vragen om hun aanbevolen uitsluitingen toe te voegen, dit zorgt ervoor dat het beveiligde eindpunt en de AV tegelijkertijd kunnen functioneren en ook de impact op de prestaties tot een minimum beperken.

Onduidelijke uitsluitingen

Aanbevolen wordt een dubbel beleid te maken om problemen op het gebied van bedrijfsbeveiliging en verstoringen te voorkomen, om computers met prestatie-indicatoren te identificeren en ze in een groep te scheiden om dit duplicaat-beleid te gebruiken.

> **Waarschuwing**: configuratiewijzigingen op het dashboard vereisen tijd om connectors toe te staan het beleid te synchroniseren. Laat een hartslag update toe of synchroniseer handmatig het beleid op de connectors.

Beleidsvorming

1. **Secure Endpoint console > tabblad Beheer > Beleid**
2. Klik op **+ Nieuw beleid...**
3. **Selecteer dit** in het vervolgkeuzemenu voor het besturingssysteem.
4. Geef het een zinvolle naam zodat u dit beleid en deze beschrijving kunt onderscheiden (*optioneel*).
5. Selecteer de beleidsmaatregelen om aan uw vereisten te voldoen, gebruik de standaarduitsluitingen voor nu.
6. ***Belangrijk*** In **Geavanceerde instellingen > Beheerfuncties** stelt u het logniveau van de connector in op **Debug**.
7. Klik op **Opslaan** om het maken van het beleid te voltooien.

Groepsvorming

1. **Secure Endpoint Console > tabblad Beheer > Groepen**
2. Klik op **Groep maken**
3. Geef het een betekenisvolle naam zodat u deze groep en beschrijving kunt onderscheiden (*optioneel*).
4. **Selecteer** het gedupliceerde beleid dat u hebt gemaakt.
5. Klik op **Opslaan** om het maken van de groep te voltooien.

Hoe uitsluitingen te identificeren

Na de dubbele beleid en groepsvorming, met het **debug log niveau op de connectors** voeren de *Computers* zoals bij normale zakelijke bewerkingen. Laat tijd toe om voldoende gegevens van het verbindingslogboek te verkrijgen terwijl de programma's en de processen zijn betreden, produceer een steun kenmerkende bundel om uitsluitingen te herzien en te identificeren.

Gids voor het maken van diagnostische bundels voor verschillende besturingssystemen beschikbaar:

- Windows
- Linux
- MAC

MacOS of Linux

Haal de gecomprimeerde debug diagnostische bundel. Het bestand **fileops.txt** maakt een lijst van de paden waar bestanden maken, wijzigen en hernoemen activiteiten geactiveerd Secure Endpoint om bestanden te scannen. Elk pad heeft een bijbehorende telling die aangeeft hoe vaak het gescand is en de lijst in aflopende volgorde gesorteerd wordt. Een hoog aantal betekent niet noodzakelijkerwijs dat het pad moet worden uitgesloten (een directory waarin e-mails worden opgeslagen, kan bijvoorbeeld vaak worden gescand, maar moet niet worden uitgesloten), maar de lijst biedt een startpunt om uitsluitingskandidaten te identificeren.

```
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_browsir
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
```

Windows

Het Windows-besturingssysteem is gecompliceerder en er zijn meer uitsluitingsopties beschikbaar vanwege de ouder- en kinderprocessen. Dit wijst erop dat een grondiger onderzoek vereist is om de dossiers te identificeren waartoe toegang is verkregen, maar ook de programma's die deze hebben voortgebracht. Raadpleeg deze Windows Tuning Tool op de GitHub-pagina van Cisco Security voor meer informatie over het analyseren en optimaliseren van Windows-prestaties met Secure Endpoint.

Hoe te om Uitsluitingen te creëren

Deze sectie behandelt de beste praktijken om uitsluitingen voor uw milieu te schrijven.

> **Waarschuwing**: begrijp altijd de bestanden en processen voordat u een uitsluiting schrijft om beveiligingskwetsbaarheden voor de computer te voorkomen.

> **Opmerking**: Aanvullende informatie is beschikbaar in de Gebruikersgids, hoofdstuk 3 hier bekijken. Dit hoofdstuk behandelt de soorten uitsluitingen, implementatie en navigatie van het beveiligde endpointportaal.

CSIDL-pad en -proces

CSIDL is een geaccepteerde en bemoedigde manier om uitsluitingen te schrijven. CSIDL maakt procesuitsluitingen mogelijk die kunnen worden bevestigd in omgevingen die alternatieve aandrijfletters gebruiken en die de noodzaak van een jokerteken kunnen omzeilen wanneer dat pad gebruikerspecifiek is (omdat procesuitsluitingen geen jokerteken toestaan). Meer informatie over CSIDL . Er zijn echter beperkingen waarmee rekening moet worden gehouden bij het gebruik van CSIDL. Als uw omgeving programma's op meer dan één stationsaanduiding installeert, verwijst het CSIDL-pad alleen naar het station dat als de standaardinstallatielocatie is gemarkeerd, bijvoorbeeld als het besturingssysteem is geïnstalleerd op C:\ maar het installatiepad voor Microsoft SQL handmatig is gewijzigd in D:\, dan is de op CSIDL-gebaseerde uitsluiting in de lijst met onderhouden uitsluitingen niet van toepassing op dat pad. Voor procesuitsluitingen betekent dit dat voor elk proces dat niet op het C:\ station staat, één uitsluiting moet worden ingevoerd omdat het gebruik van CSIDL dit niet in kaart brengt.

Uitsluitingen pad

Deze uitsluitingen zijn de meest gebruikte, applicatie conflicten meestal impliceren de uitsluiting van een directory. Maak een pad uitsluiting met een absoluut pad of de CSIDL.

Als u bijvoorbeeld een antivirustoepassing in de map Program Files wilt uitsluiten, is het uitsluitingspad:

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

Zonder een achterliggende slash past de **Windows-connector** een gedeeltelijke match op paden, terwijl **Mac en Linux dat niet doen.**

Voorbeeld als u de volgende Path-uitsluitingen"**C:\Program Files"** en als **"C:\test" toepast:**

C:\Program Bestanden en **C:\Program Bestanden (x86)** zijn uitgesloten:

<#root>

```
C:\Program Files
```

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

C:\test is uitgesloten, zoals **C:\test123**:

<#root>

```
C:\test
```

```
C:\test123
```

U kunt de uitsluiting van "**C:\test"** in "**C:\test\"** wijzigen, dit voorkomt dat "**C:\test123"** wordt uitgesloten.

Opmerking: Path Exclusions zijn recursief en sluiten alle subdirectory's ook uit.

Bestandsextensie

Deze uitsluitingen maken het mogelijk alle bestanden met een bepaalde extensie uit te sluiten.

Belangrijkste punten:

- Verwacht invoersignaal aan de aansluitzijde is **.extension**
- Het Dashboard maakt automatisch een punt voor de bestandsextensie als er geen toegevoegd is.
- Uitbreidingen zijn ***niet*** hoofdlettergevoelig.

U kunt bijvoorbeeld de volgende uitsluiting maken om alle Microsoft Access-databasebestanden uit te sluiten:

```
.MDB
```

Opmerking: standaarduitsluitingen zijn beschikbaar in de standaardlijst. Het is **niet** aanbevolen om deze uitsluitingen te verwijderen. Dit kan leiden tot prestatiewijzigingen op uw *computers.*

---

jokerteken

Deze uitsluitingen zijn hetzelfde als pad- of extensie-uitsluitingen, behalve wanneer een sterretje (*) wordt gebruikt als een jokerteken.

> **Waarschuwing**: uitsluiting van jokerteken stopt niet bij padscheidingstekens, dit kan leiden tot onbedoelde uitsluitingen. Voorbeeld: **C:*\test** sluit **C:\sample\test** en **C:\1\test** of **C:\sample\test123 uit.**

> **Waarschuwing**: een uitsluiting starten met een sterretje(*) kan grote problemen met de prestaties veroorzaken. Met **7.5.3+** veroorzaakte de toevoeging van Uitsluitingen van het Wildkaartproces extra prestatieproblemen met uitsluiting van sterretjes. Verwijder of wijzig alle uitsluitingen in deze bestandsindeling om het cpu-effect te beperken.

Als u bijvoorbeeld virtuele machines op een MAC uitsluit van scannen, moet u dit pad uitsluiten:

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

Deze uitsluiting werkt alleen voor *johndoe*, om meerdere gebruikersovereenkomsten toe te staan, de gebruikersnaam in het pad vervangen door een asterisk(*) door een uitsluiting met johndoe-wildcard:

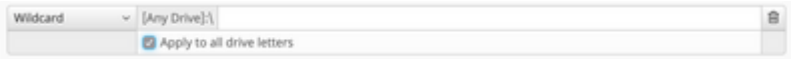
```
/Users/*/Documents/Virtual Machines/
```

Schrijf een uitsluiting voor paden die in afzonderlijke stations bestaan.

Bijvoorbeeld: **C:\testpath** en **D:\testpath** zijn:

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

Het systeem genereert automatisch de ^[A-Z-z] wanneer "Apply to all drive letters" wordt gecontroleerd nadat de wildcard is geselecteerd in de uitrollijst Type uitsluiting, zoals in de afbeelding:



Proces

Procesuitsluitingen stellen beheerders in staat lopende processen uit te sluiten van normale bestandsscans (Secure Endpoint Windows Connector, versie 5.1.1 en hoger), systeemprocesbescherming (Connector, versie 6.0.5 en hoger) of bescherming tegen kwaadaardige activiteit (Connector, versie 6.1.5 en hoger).

Procesuitsluiting wordt uitgevoerd door: het specificeren van het volledige pad naar het uitvoerbare proces, de SHA-256 waarde van het uitvoerbare proces, of zowel het pad als de SHA-256. Paden staan beide directe paden toe of gebruiken een CSIDL-waarde.

> **Voorzichtig**: Kinderprocessen die door een uitgesloten proces worden gecreëerd, worden **niet**

---

standaard in de uitsluiting opgenomen. Voorbeeld: Procesuitsluiting voor MS Word zou standaard geen extra processen uitsluiten die door Word.exe zijn gemaakt en zou worden gescand. Als u extra processen wilt opnemen, klikt u op het selectievakje **Kinderprocessen toepassen**. Verder, wordt het uitsluiten van Word.exe niet gesuggereerd aangezien malware regelmatig verbergt in moderne .docx bestanden.

Opmerking: zowel pad als SHA-256 opgeven is vereist om het proces uit te sluiten als aan beide voorwaarden wordt voldaan.

Beperkingen:

- Als de bestandsgrootte van het proces groter is dan de maximale grootte van een scanbestand die in uw beleid is ingesteld, dan wordt de SHA-256 van het proces niet berekend en **werkt** de uitsluiting **niet**. Gebruik een pad-gebaseerde procesuitsluiting voor bestanden die groter zijn dan de maximale grootte van een scanbestand.
- Connectorversies 5.x.x tot 6.0.3 - een limiet van 25 procesuitsluitingen voor alle procesuitsluitingstypen
- Connectorversies 6.0.5+ - limiet van 100 procesuitsluitingen voor alle procesuitsluitingstypen.
- Connectorversies 7.x.+ - limiet van 500 procesuitsluitingen voor alle procesuitsluitingstypen.
- De connector respecteert alleen de procesuitsluitingen tot aan de limiet, vanaf de bovenkant van de lijst met procesuitsluitingen in policy.xml
- Elk beleid heeft een procesuitsluiting voor sfc.exe, die telt tegen de limiet

```
3|0||CSIDL_Secure Endpoint_VERSION\sfc.exe|48|
```

dreigement

Deze uitsluitingen maken het mogelijk dat een bepaalde bedreigingsnaam wordt uitgesloten van het veroorzaken van gebeurtenissen. Bedreigingsuitsluiting mag alleen worden gebruikt wanneer het scanresultaat aanleiding geeft tot vals-positieve detectie en bevestigd wordt dat ze geen echte bedreiging vormen.

Tekstvak om een uitsluiting van een bedreiging toe te voegen is ***niet*** hoofdlettergevoelig. Voorbeeld: W32.Zombies.NotAVirus of w32.zombies.notavirus hebben beide dezelfde bedreigingsnaam.

Waarschuwing: sluit bedreigingen niet uit, tenzij onderzoek en bevestiging van de bedreigingsnaam als vals positief worden beschouwd. Uitgesloten bedreigingen worden niet langer ingevuld in het tabblad gebeurtenissen voor review en audit.

Verwerkingsjokerteken

Windows

Endpoint 7.5.3+ staat extra uitsluitingen toe met behulp van de functionaliteit voor jokerteken binnen de Procesuitsluitingen. Dit maakt een bredere dekking mogelijk met minder uitsluitingen, maar kan ook gevaarlijk zijn als te veel ongedefinieerd blijft. **U mag de jokerteken alleen gebruiken om het minimum aantal tekens te dekken dat nodig is om de gewenste uitsluiting op te geven.**

Gebruik van (*) in Process Wildcard voor Windows:

- (*) Kan worden gebruikt in plaats van één teken of een volledige map. Dit kan niet aan het begin van het pad worden geplaatst, het wordt ongeldig verklaard. De jokerteken werkt tussen twee gedefinieerde tekens, schuine strepen of alfanumerieke tekens. Het plaatsen van het aan het eind van een pad zal de processen in die map uitsluiten, maar niet subdirectories.
- (**) Kan aan het eind van een pad worden gebruikt om alle processen in die map en de processen in de subdirectory's uit te sluiten. Dit zorgt voor een veel grotere uitsluiting set met minimale input, maar laat ook een zeer groot veiligheidsgat voor zichtbaarheid. **Gebruik deze functie met uiterste voorzichtigheid**.

Voorbeelden:

```
C:\Windows\*\Tiworker.exe - Excludes all Tiworker.exe found in the subfolders of 'Windows'
C:\Windows\P*t.exe - Excludes Pot.exe, Pat.exe, P1t.exe Etc.
C:\Windows\*chickens.exe - Excludes all Processes in 'Windows' folder ending in chickens.exe
C:\* - Excludes all Processes in the C: drive in the top layer of folders but not the subfolders
C:\** - Excludes every Process on the C: drive.
```

MacOS en Linux

Endpoint 1.15.2+ staat extra uitsluitingen toe met behulp van de functionaliteit voor jokerteken binnen de Procesuitsluitingen. Dit maakt een bredere dekking mogelijk met minder uitsluitingen, maar kan ook gevaarlijk zijn als te veel ongedefinieerd blijft. **U mag de jokerteken alleen gebruiken om het minimum aantal tekens te dekken dat nodig is om de gewenste uitsluiting op te geven.**

Gebruik van (*) in Proces Wildcard voor Mac:

- (*) Kan worden gebruikt in plaats van één teken of een volledige map. Dit kan niet aan het begin van het pad worden geplaatst, het wordt ongeldig verklaard. De jokerteken werkt tussen twee gedefinieerde tekens, schuine strepen of alfanumerieke tekens.

Voorbeelden:

```
/Library/Java/JavaVirtualMachines/*/java - Excludes Java within all subfolders of JavaVirtualMac
/Library/Jibber/j*bber - Excludes the Process for jabber, jibber, jobber, etc.
```

Uitsluitingen ter voorkoming van exploitatie (toepassing)

Windows

Secure Endpoint 7.5.1+ maakt gebruik van V5 van de Exploit Prevention Engine en de console maakt het nu mogelijk om uitsluitingen van toepassingen te configureren binnen de huidige functionaliteit van de uitsluitingslijst. **Dit is momenteel beperkt tot toepassingen en alle uitsluitingen met betrekking tot DLL's moeten nog steeds worden gedaan door het openen van een case met ondersteuning.**

Het vinden van de juiste uitsluitingen voor Exploit Prevention is een veel intensiever proces dan elk ander uitsluitingstype en vereist uitgebreide tests om schadelijke beveiligingsgaten te minimaliseren.

Gemeenschappelijke te vermijden fouten

Gebruik voorzichtigheid bij het maken van uitsluitingen, omdat dit het beschermingsniveau verlaagt dat wordt geboden door Cisco Secure Endpoint. Uitgesloten bestanden worden niet gehakt, gescand of beschikbaar in de cache of cloud, activiteit wordt niet gecontroleerd en informatie ontbreekt in Backend Engines, Device Trajectory en Advanced Analysis.

Uitsluitingen mogen *alleen* spaarzaam worden gebruikt in specifieke gevallen zoals compatibiliteitskwesties met specifieke toepassingen of prestatieproblemen die niet op een andere manier kunnen worden verbeterd.

Hieronder staan enkele veelvoorkomende fouten die vermeden moeten worden bij het werken met uitsluitingen.

- **Proactieve uitsluitingen**
  - Ga er niet van uit dat uitsluiting noodzakelijk is tenzij is aangetoond dat het een probleem is dat niet op een andere manier kan worden aangepakt. Prestatieproblemen, fout-positieven of problemen met de compatibiliteit van toepassingen moeten grondig worden onderzocht en verzacht voordat een uitsluiting wordt toegepast

- **Een te ruime uitsluiting**
  - Het uitsluiten van grote delen van het eindpunt, zoals het gehele C-station
  - Een uitsluiting van een jokerteken gebruiken als een meer specifieke uitsluiting mogelijk is
  - Alleen de bestandsnaam gebruiken in plaats van een volledig gekwalificeerd pad naar het bestand
  - Gebruik Device Trajectory of Secure Endpoint Diagnostics Package en Performance Tuning Tool om de specifieke uitsluiting te onderzoeken en te bepalen die nodig is

- **Overmatig gebruik van uitsluiting van jokerteken**
  - Uitsluitingen van jokertekens creëren niet alleen meer beveiligingshiaten, maar vereisen ook meer systeembronnen dan elk ander type uitsluiting
  - Zorg ervoor dat u de minimale hoeveelheid jokertekens in een uitsluiting gebruikt; alleen de mappen die echt variabel zijn, moeten variabel worden gemaakt met een jokerteken. Voorbeeld:
    - Software* zal alles in de map uitsluiten, maar niet de submappen.
    - Software** van het programma sluit alles in de map, inclusief submappen, uit

- **Met uitzondering van artikelen die bij aanvallen worden gebruikt**
  - Bestandstypen zoals .cmd, .zip, .jpg, enz
  - Processen zoals svchost.exe, bash.exe, powershell.exe, enz.
  - Mappenlocaties zoals C:\Users\, C:\Windows\Temp\, C:\Program Files\Java, etc

- **Dubbele uitsluitingen**
  - Controleer voordat u een uitsluiting maakt of de uitsluiting al bestaat in de door de gebruiker gemaakte aangepaste uitsluitingen of in de door Cisco onderhouden uitsluitingen.
  - Het verwijderen van dubbele uitsluitingen verbetert niet alleen de prestaties maar vermindert ook het operationele beheer van uitsluitingen

- **Verouderde uitsluitingen**
  - Uitsluitingen die al lang geleden zijn gecreëerd en misschien nog niet nodig zijn.
  - Beoordeel en controleer regelmatig uw uitsluitingslijst en zorg ervoor dat u een register bijhoudt van de redenen waarom een bepaalde uitsluiting is toegevoegd.

- **Niet verwijderen van uitsluitingen na infectie**
  - Uitsluitingen moeten worden verwijderd zodra een infectie is vastgesteld om optimale veiligheid en zichtbaarheid te herstellen
  - Met behulp van de functie "Computer naar groep verplaatsen" vooraf kunt u snel een veiliger beleid na infectie toepassen, inclusief het instellen van een beleid zonder enige uitsluitingen

- **Gebrek aan tactieken om de gevolgen te beperken**
  - Als uitsluitingen absoluut noodzakelijk zijn, overweeg dan welke verzachtende tactiek kan worden toegepast, zoals het in staat stellen van schrijfbeveiliging om wat extra beschermingslagen toe te voegen voor de uitgesloten items.

Zie de handleiding met best practices voor meer informatie over uitsluitingen of beveiligde endpoints

Uitsluitingen niet aanbevolen

Voor een goede veiligheidshouding en zichtbaarheid worden de volgende uitsluitingen niet aanbevolen:

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
iexplorer.exe
java.exe
kd.exe
lxsmanager.dll
msbuild.exe
mshta.exe
ntkd.exe
ntsd.exe
outlook.exe
psexec.exe
powerpnt.exe
powershell.exe

rcsi.exe
svchost.exe
schetaken.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
1,934 kW
.py
.rar

.reg
.scr
sys. sys
.tar
.tmp
.url
.vbe
.vbs
.wsf
.zip
opdoffer
java
python
python3
sh
sjiek
/
/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 Bestanden\<bedrijfsnaam>\
C:\Program Bestanden (x86)\<bedrijfsnaam>\
C:\Users\<UserProfileName>\AppData\Local\Temp\
C:\Users\<UserProfileName>\AppData\LocalLow\Temp\

Gerelateerde informatie

- **Technische ondersteuning en documentatie â€“ Cisco Systems**
- **Cisco Secure Endpoint - TechNotes**
- **Cisco Secure Endpoint - gebruikershandleiding**
- **Secure Endpoint: procesuitsluitingen in macOS en Linux**

Over deze vertaling

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