

Wijzigingen in Cisco Secure Endpoint console voor onderhoud van uitsluitingslijst

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Verwachtingen bij het bijwerken](#)

[Wijzigingen](#)

[28 augustus - 2019](#)

[Standaard Microsoft Windows:](#)

[N-Able Solar Winds - Windows:](#)

[Docker - Mac:](#)

[Nieuwe lijsten gemaakt:](#)

[18 september - 2019](#)

[Standaard Apple MacOS:](#)

[McAfee - Mac](#)

[Cisco Jabber - Mac](#)

[Crashplan - Mac](#)

[JAMF Casper - Mac](#)

[VMWare Fusion - Mac](#)

[Xcode - Mac](#)

[One Drive - Windows](#)

[Citrix SCA-client - Windows](#)

[Nieuwe lijsten gemaakt:](#)

[11 december - 2019](#)

[One Drive - Windows](#)

[Splunk - Windows](#)

[Splunk - Linux](#)

[Nieuwe lijsten gemaakt:](#)

[12 februari - 2020](#)

[Standaard Microsoft Windows - Windows](#)

[Websense - Windows](#)

[Microsoft SQL Server - Windows](#)

[10 juni - 2020](#)

[Malwarebytes - Windows](#)

[Microsoft Office - Windows](#)

[IIS - Windows](#)

[Altiris van Symantec - Windows](#)

[McAfee - Windows](#)

[Nieuwe lijsten gemaakt:](#)

[15 juli - 2020](#)

[Domain Controllers - Windows](#)

[Microsoft Teams - Windows](#)

[Nieuwe lijst gemaakt](#)

[26 augustus - 2020](#)

[Microsoft SQL Server - Windows](#)

[30 september - 2020](#)

[Malwarebytes - Windows](#)

[Digitale Guardian - Mac](#)
[Nieuwe lijst gemaakt](#)
[3 maart - 2021](#)
[Kaspersky - Windows](#)
[SCM - Windows](#)
[Symantec - Windows](#)
[Nieuwe lijsten gemaakt](#)
[30 juni - 2021](#)
[Standaard Microsoft Windows](#)
[Citrix SCA-client](#)
[Citrix Provisioning Server](#)
[Nieuwe lijsten gemaakt](#)
[29 september - 2021](#)
[Cisco Webex - Windows](#)
[Crashplan - Windows](#)
[Crashplan - Mac](#)
[VMware - Windows](#)
[23 maart - 2022](#)
[Standaard Microsoft Windows](#)
[Hyper-V - Windows](#)
[Microsoft Windows Defender - Windows](#)
[29 juni - 2022](#)
[Standaard Microsoft Windows](#)
[Cisco AnyConnect VPN](#)
[Cisco Webex](#)
[Microsoft OneDrive \(voorheen één station\)](#)
[Tanium - Windows](#)
[Citrix Provisioning Server](#)
[Nieuwe lijsten gemaakt](#)
[14 september - 2022](#)
[Standaard Microsoft Windows](#)
[Microsoft SQL Server](#)
[TrendMicro/Apex One](#)
[Nieuwe lijsten gemaakt](#)
[Oktober - 2022](#)
[14 december - 2022](#)
[Standaard Microsoft Windows](#)
[Veranderingen in backend - Windows](#)
[Nieuwe lijsten gemaakt](#)
[12 april - 2023](#)
[Standaard Microsoft Windows](#)
[Microsoft Intune](#)
[McAfee Trellix SolidCore](#)
[Cisco Webex](#)
[Microsoft Defender voor MacOS](#)
[Microsoft Defender voor Linux](#)
[31 mei - 2023](#)
[VEEAM](#)
[VMWare](#)

Inleiding

Dit document beschrijft de wijzigingen die zijn toegevoegd aan de door Cisco beheerde uitsluitingen.

Uitsluitingen met Cisco-onderhoud worden gemaakt en onderhouden door Cisco om een betere compatibiliteit te bieden tussen de Advanced Malware Protection (AMP) voor Endpoints Connector en antivirus-, security- of andere software. Deze uitsluitingen kunnen worden toegevoegd aan nieuwe versies van een toepassing.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Uitsluitingen in Advanced Malware Protection voor endpoints
- AMP-console

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- AMP voor endpoints, versie 5.4.20190820

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.

Verwachtingen bij het bijwerken

The screenshot shows the Cisco AMP for Endpoints interface. At the top, the Cisco logo and 'AMP for Endpoints' are visible. Below the navigation bar (Dashboard, Analysis, Outbreak Control, Management, Accounts), the 'Exclusions' section is active. It features two tabs: 'Custom Exclusions' and 'Cisco-Maintained Exclusions'. A tooltip points to the 'Cisco-Maintained Exclusions' tab with the text: 'Cisco-Maintained Exclusions are maintained by Cisco to provide better compatibility between the AMP for Endpoints Connector and antivirus or other software. These exclusions are updated with improvements and new exclusions may be added for new applications.' Below the tabs is a search bar with the placeholder text 'Search by exclusion set, path, extension, threat name, or SHA-256'. At the bottom, there are four filter buttons: 'All Products', 'Windows', 'Mac', and 'Linux'.

Wanneer de door Cisco onderhouden lijsten worden gewijzigd, vindt er een beleidsupdate plaats op de backend om die wijziging weer te geven. Aangezien elk van de Endpoints die lijst gebruikt incheckt op hun hartslag, trekken zij het bijgewerkte beleid. Deze beleidswijzigingen worden niet weerspiegeld in het controlelogboek, aangezien het technisch een wijziging in de uitsluitingslijst is, niet het beleid zelf, en de door Cisco onderhouden uitsluitingslijsten bestaan niet binnen de normale controlelogboeken op individuele consoles. Voor grootschalige omgevingen ziet dit eruit als een stroom van beleidsupdates en het eindresultaat zal betere prestaties zijn op elk van de Endpoints.

De updateperiode hangt af van elk eindpunt. Als alle machines online zijn, zouden de updates plaatsvinden binnen 1-2 hartslagen. Als dit een wereldwijde omgeving is, blijven updates voorkomen als machines online komen, dus wees niet verrast om extra

beleidsupdates te zien 24-48 uur nadat de lijst met onderhouden wordt gedrukt.

Wijzigingen

28 augustus - 2019

Standaard Microsoft Windows:

Verwijdering van:

- **CSIDL_WINDOWS\SoftwareDistribution\Datastore\Logs\edb*.log**
- **CSIDL_WINDOWS\SoftwareDistribution\Datastore\Logs\Res1.log**
- **CSIDL_WINDOWS\SoftwareDistribution\Datastore\Logs\Res2.log**

Reden: repetitief. Een andere uitsluiting in het basisstel dekt het.

toevoeging van:

- **C:\\$WINDOWS.~BT\Sources\SetupHost.exe**

Reden: Windows 10-updates faalden sporadisch als gevolg van processcans.

N-Able Solar Winds - Windows:

toevoeging van:

- **C:\Program Files (x86)\N-able Technologies\Windows Agent\bin\agent.exe**
- **C:\Program Files (x86)\BeAnywhere Support Express\GetSupportService_N-Central\BASupSrv.exe**
- **C:\Program Files (x86)\N-able Technologies\PatchManagement\ThirdPartyPatch\ThirdPartyPatch.exe**

Docker - Mac:

Verwijdering van:

- **/Gebruikers/*/Library/Containers/com.docker.docker/Data/vms/*/Docker.***
- **/usr/local/bin/docker**

Reden: Aanvullende tests hebben ons zorgen gemaakt over de veiligheid, dus de ontwikkeling heeft betere uitsluitingen aan het licht gebracht.

toevoeging van:

- **/Applications/Docker.app/Contents/MacOS/Docker**
- **/Applications/Docker.app/Contents/Resources/bin/docker**

Nieuwe lijsten gemaakt:

Linux:

- Docker - Connector 1.10.2
- Docker - Connector 1.1+
- Zabbix

Mac:

- Virtueel vak
- Digitale bewaker

18 september - 2019

Standaard Apple MacOS:

toevoeging van:

- **/Toepassingen/Tijdmachine.app/Inhoud/MacOS/Tijdmachine**
- **/System/Library/CoreServices/Spotlight.app/Contents/MacOS/Spotlight**

McAfee - Mac

toevoeging van:

- **/Library/McAfee/Agent/bin/CmdAgent**

Cisco Jabber - Mac

Verwijdering van:

- **/usr/bin/grep**
- **/bin/ps**

Reden: Betere beveiliging en de extra functionaliteit van procesgebaseerde uitsluitingen.

toevoeging van:

- **/Toepassingen/Cisco Jabber.app/Content/MacOS/Cisco Jabber**

Crashplan - Mac

toevoeging van:

- **/Applications/CrashPlan.app/Contents/Library/LaunchServices/CrashPlanService.app/Contents/MacOS/CrashPlanService**

JAMF Casper - Mac

Verwijdering van:

- **/usr/bin/sw_ers**

Reden: Betere beveiliging en de extra functionaliteit van procesgebaseerde uitsluitingen.

toevoeging van:

- **/Library/Application Support/JAMF/Jamf.app/Contents/MacOS/JamfDaemon.app/Contents/MacOS/JamfDaemon**
- **/usr/local/jamf/bin/jamfAgent**
- **/usr/local/jamf/bin/jamf**
- **/Library/Application Support/JAMF/Jamf.app/Contents/MacOS/JamfAgent.app/Contents/MacOS/JamfAgent**

VMWare Fusion - Mac

toevoeging van:

- **/Toepassingen/VMware Fusion.app/Contents/MacOS/VMware Fusion**

Xcode - Mac

toevoeging van:

- **/Applications/Xcode.app/Contents/SharedFrameworks/XCBuild.framework/Versions/A/PlugIns/XCBuildService.bundle/Contents/Resources/xcodesign**
- **/Applications/Xcode.app/Contents/Developer/usr/bin/xcodesign**

One Drive - Windows

Kleine wijziging:

- **C:*\\Users\\OneDrive** (Voeg de backslash toe voor een betere beveiliging)

Citrix MICA-client - Windows

toevoeging van:

- **CSIDL_PROGRAM_FILES\Citrix\User Profile Manager\UserProfileManager.exe**
- **CSIDL_PROGRAM_FILES\Citrix\Virtual Desktop Agent\BrokerAgent.exe**
- **CSIDL_PROGRAM_FILES\Citrix\ICAService\picaSvc2.exe**
- **CSIDL_PROGRAM_FILES\Citrix\ICAService\CpSvc.exe**

Reden: Recente update van Citrix suggereerde uitsluitingen.

Nieuwe lijsten gemaakt:

Windows

- Citrix Provisioning Server
- Citrix Cloud-connector

11 december - 2019

One Drive - Windows

toevoeging van:

- **CSIDL_LOCAL_APPDATA\Microsoft\OneDrive\OneDrive.exe**

Splunk - Windows

toevoeging van:

- **CSIDL_PROGRAM_FILE\splunkforwarder\bin\splunk-winevtlog.exe**
- **CSIDL_PROGRAM_FILE\splunkforwarder\bin\splunkd.exe**

Splunk - Linux

toevoeging van:

- **/opt/splunkforwarder/bin/splunk**
- **/opt/splunk/bin/splunk**

Nieuwe lijsten gemaakt:

Azure - Linux

Vagrant - Mac

12 februari - 2020

Standaard Microsoft Windows - Windows

toevoeging van:

- **C:\Program Files\Cisco\Orbital\osqueryd.exe**
- **C:\Program Files\Cisco\Orbital\orbital-ampwin.exe**

Websense - Windows

toevoeging van:

- **[Meerdere stations]:\Program Files*\Websense**
- **C:\Program Bestanden (x86)\Websense\Websense-eindpunt\dserui.exe**
- **C:\Program Files\Websense\Websense Endpoint\dserui.exe**
- **C:\Program Bestanden (x86)\Websense\Websense-eindpunt\EndPointClassifier.exe**
- **C:\Program Bestanden (x86)\Websense\Websense\FilterSDK\kvoop.exe**
- **C:\Program Bestanden (x86)\Websense\Websense-endpoint\wepsvc.exe**

Microsoft SQL Server - Windows

toevoeging van:

- **CSIDL_PROGRAM_FILES\Microsoft SQL Server\MSSQL\FTDATA**
- **.sql**

10 juni - 2020

Malwarebytes - Windows

Kleine wijziging:

- **C:\ProgramData\Malwarebytes Endpoint Agent**
- **C:\ProgramData\Malwarebytes\MBAMService**

Microsoft Office - Windows

toevoeging van:

- **C:\Program Files\Common Bestanden\microsoft gedeeld\ClickToRun\OfficeClickToRun.exe**

IIS - Windows

toevoeging van:

- **C:\Windows\SysWOW64\inetsrv\w3wp.exe**
- **C:\Windows\System32\inetsrv\w3wp.exe**

Altiris van Symantec - Windows

toevoeging van:

- **C:\Program Files\Altiris\Altiris Agent\AeXNgent.exe**

McAfee - Windows

toevoeging van:

- **C:\Program Files\McAfee\Endpoint Security\Adaptive Threat Protection\mfeatp.exe**

Nieuwe lijsten gemaakt:

NetScout - Windows

IBM - Windows

15 juli - 2020

Domain Controllers - Windows

toevoeging van:

- **CSIDL_WINDOWS\System32\dfsrmgr.exe**
- **CSIDL_WINDOWS\System32\dfsrs.exe**
- **CSIDL_WINDOWS\System32\dns.exe**
- **CSIDL_WINDOWS\System32\ntfrs.exe**

Microsoft Teams - Windows

toevoeging van:

- **CSIDL_LOCAL_APPDATA\Microsoft\Teams\current\teams.exe**
- **CSIDL_LOCAL_APPDATA\Microsoft\Teams\update.exe**

Nieuwe lijst gemaakt

Controle omhoog

26 augustus - 2020

**Vanwege aanvullende tests werd de oorspronkelijke introductiedatum verlengd van de 19e naar de 26e

Microsoft SQL Server - Windows

Vervangen:

- **CISCO_PROGRAMMA_FILES\Microsoft SQL Server\MSSQL.1\MSSQL\Binn\SQLServr.exe**
- **CISCO_PROGRAMMA_FILES\Microsoft SQL Server\MSSQL.2\OLAP\Bin\MSMDSrv.exe**
- **CSIDL_PROGRAM_FILES\Microsoft SQL Server\MSSQL.3\Reporting Services\ReportServer\Bin\ReportingServicesService.exe**

toevoeging van:

- **CISCO_PROGRAMMA_FILES\Microsoft SQL Server\MSSQL.11\MSSQL\Binn\SQLServr.exe**
- **CISCO_PROGRAMMA_FILES\Microsoft SQL Server\MSSQL.12\MSSQL\Binn\SQLServr.exe**
- **CISCO_PROGRAMMA_FILES\Microsoft SQL Server\MSSQL.13\MSSQL\Binn\SQLServr.exe**
- **CISCO_PROGRAMMA_FILES\Microsoft SQL Server\MSSQL.11\OLAP\Bin\MSMDSrv.exe**
- **CISCO_PROGRAMMA_FILES\Microsoft SQL Server\MSSQL.12\OLAP\Bin\MSMDSrv.exe**
- **CISCO_PROGRAMMA_FILES\Microsoft SQL Server\MSSQL.13\OLAP\Bin\MSMDSrv.exe**
- **CSIDL_PROGRAM_FILES\Microsoft SQL Server\MSSQL.11\Reporting Services\ReportServer\Bin\ReportingServicesService.exe**
- **CSIDL_PROGRAM_FILES\Microsoft SQL Server\MSSQL.12\Reporting Services\ReportServer\Bin\ReportingServicesService.exe**
- **CSIDL_PROGRAM_FILES\Microsoft SQL Server\MSSQL.13\Reporting Services\ReportServer\Bin\ReportingServicesService.exe**

30 september - 2020

Malwarebytes - Windows

toevoeging van:

- **CSIDL_PROGRAM_FILES\Malwarebytes' Anti-Malware\mbam.exe**
- **CSIDL_PROGRAM_FILES\X86\Malwarebytes' anti-Malware\mbam.exe**

Digitale Guardian - Mac

toevoeging van:

- **/usr/local/dgagent**
- **/dgagent**

Nieuwe lijst gemaakt

Digital Guardian - Windows

3 maart - 2021

Kaspersky - Windows

toevoeging van:

- **CSIDL_PROGRAM_FILES\X86\Kaspersky Lab\Kaspersky Endpoint Security for Windows\avp.exe**
- **CSIDL_PROGRAM_FILES\X86\Kaspersky Lab\NetworkAgent\klnagent.exe**

SCM - Windows

Verwijdering van:

- **WINDOWS\CCM\ServiceData** - Dubbele pad
- **Program Files\Microsoft Configuration Manager\EasySetuppayload** - Duplicate Path

Symantec - Windows

toevoeging van:

- **CSIDL_PROGRAM_FILES\Symantec\Endpoint Agent\edpa.exe**
- **CSIDL_PROGRAM_FILESX86\Symantec\Symantec Endpoint Protection\12.1.4013.4013.105\Bin64\Smc.exe**
- **CSIDL_PROGRAM_FILESX86\Symantec\Symantec Endpoint Protection\12.1.608.6300.105\Bin\ccSvcHst.exe**
- **CSIDL_PROGRAM_FILESX86\Symantec\Symantec Endpoint Protection\12.1.7061.600.105\Bin\ccSvcHst.exe**
- **CSIDL_PROGRAM_FILESX86\Symantec\Symantec Endpoint Protection\12.1.7385.6902.105\Bin\ccSvcHst.exe**
- **CSIDL_PROGRAM_FILESX86\Symantec\Symantec Endpoint Protection**
- **CSIDL_PROGRAM_FILES\Symantec\Endpoint Agent\brkrprcs64.exe**

Nieuwe lijsten gemaakt

Cisco AnyConnect - Windows

Microsoft Defender ATP - Windows

30 juni - 2021

Standaard Microsoft Windows

toevoeging van:

- **CSIDL_WINDOWS\System32\GroupPolicy\User\registry.pol**
- **CSIDL_WINDOWS\System32\GroupPolicy\Machine\registry.pol**

Citrix SCA-client

toevoeging van:

- **CSIDL_PROGRAM_FILES\Citrix\Broker\Service\BrokerService.exe**
- **CSIDL_PROGRAM_FILES\Citrix\Broker\Service\HighAvailabilityService.exe**
- **CSIDL_PROGRAM_FILES\Citrix\ConfigSync\ConfigSyncService.exe**
- **CSIDL_PROGRAM_FILESX86\Citrix\ICA-client**

Citrix Provisioning Server

Verwijdering van:

- **C:\System32\drivers\CfsDep2.sys**
- **C:\System32\drivers\CvhdBusP6.sys**
- **C:\System32\drivers\CVhdMp.sys**

toevoeging van:

- CSIDL_WINDOWS\System32\drivers\CfsDep2.sys
- CSIDL_WINDOWS\System32\drivers\CvhdBusP6.sys
- CSIDL_WINDOWS\System32\drivers\CVhdMp.sys
- CSIDL_PROGRAM_FILES\Citrix\Provisioning Services\BNTFTP.EXE
- CSIDL_PROGRAM_FILES\Citrix\Provisioning Services\PVSTSB.EXE
- CSIDL_PROGRAM_FILES\Citrix\Provisioning Services\StreamService.exe
- CSIDL_PROGRAM_FILES\Citrix\Provisioning Services\StreamProcess.exe
- CSIDL_PROGRAM_FILES\Citrix\Provisioning Services\soapserver.exe
- CSIDL_PROGRAM_FILES\Citrix\Provisioning Services\Inventory.exe
- CSIDL_PROGRAM_FILES\Citrix\Provisioning Services\Notifier.exe
- CSIDL_PROGRAM_FILES\Citrix\Provisioning Services\MgmtDaemon.exe
- CSIDL_PROGRAM_FILES\Citrix\Provisioning Services\BNPXE.exe
- CSIDL_PROGRAM_FILES\Citrix\Provisioning Services\BNDevice.exe

Nieuwe lijsten gemaakt

Comprimering - Windows

Citrix Sessions Recording - Windows

29 september - 2021

Cisco Webex - Windows

toevoeging van:

- CSIDL_LOCAL_APPDATA\CiscoSparkLauncher\CiscoCollabHost.exe
- CSIDL_LOCAL_APPDATA\CiscoSparkLauncher\
- CSIDL_LOCAL_APPDATA\WebEx\WebEx\Meetings_01\atmgr.exe
- CSIDL_LOCAL_APPDATA\WebEx\WebEx\Meetings_02\atmgr.exe
- CSIDL_LOCAL_APPDATA\WebEx\WebEx\Meetings_03\atmgr.exe
- CSIDL_LOCAL_APPDATA\WebEx\WebEx\Meetings_04\atmgr.exe
- CSIDL_LOCAL_APPDATA\WebEx\WebEx\Meetings_*

Crashplan - Windows

toevoeging van:

- CSIDL_PROGRAM_FILES\Code42\Code42Service.exe

Crashplan - Mac

toevoeging van:

- /Applications/Code42.app/Contents/Library/LaunchServices/Code42Service.app/Contents/MacOS/Cod

VMware - Windows

toevoeging van:

- CSIDL_PROGRAM_FILESX86\VMware\VMware DataS Agent\service\DaaGent.exe

23 maart - 2022

Standaard Microsoft Windows

toevoeging van:

- **C:\Windows\System32\SearchIndexer.exe**

Hyper-V - Windows

toevoeging van:

- **CSIDL_COMMON_APPDATA\Microsoft\Windows\Hyper-V**
- **CSIDL_COMMANDO_DOCUMENTEN\Hyper-V\Virtual Hard Disks**

Microsoft Windows Defender - Windows

toevoeging van:

- ***\ProgramData\Microsoft\Windows Defender Advanced Threat Protection\DataCollection**

29 juni - 2022

Standaard Microsoft Windows

toevoeging van:

- ***.applocker**

Cisco AnyConnect VPN

toevoeging van:

- **CSIDL_PROGRAM_FILESX86\Cisco\Cisco AnyConnect Secure Mobility Client\acwebhelper.exe**

Cisco Webex

toevoeging van:

- **C:\Users*\AppData\Local\WebEx\WebEx\Meetings\atmgr.exe**

Microsoft OneDrive (voorheen één station)

toevoeging van:

- **C:\Users*\AppData\Local\Microsoft\OneDrive\OneDrive.exe**

Tanium - Windows

toevoeging van:

- **C:\Program Files (x86)\Tanium\Tanium End User Notification Tools\bin\end-user-notifications.exe**

Citrix Provisioning Server

toevoeging van:

- **CSIDL_PROGRAM_FILES\Citrix\Provisioning Services\MgmtDaemon.com**

Verwijdering van:

- **CSIDL_PROGRAM_FILES\Citrix\Provisioning Services\MgmtDaemon.com**

Nieuwe lijsten gemaakt

X1 zoeken - Windows

Microsoft Intune - Windows

14 september - 2022

Standaard Microsoft Windows

toevoeging van:

- **CISCO_PROGRAMMA_FILESX86\CISCO\CISCO BEVEILIGDE CLIENT**
- **CSIDL_PROGRAM_FILESX86\Cisco\Cisco Secure Client\UI\acumbrellagent.exe**
- **CSIDL_PROGRAM_FILESX86\Cisco\Cisco Secure Client\UI\acumbrellagent.exencrypt-proxy.exe**
- **CSIDL_PROGRAM_FILESX86\Cisco\Cisco Secure Client\NVM\canvmagent.exe**
- **CSIDL_PROGRAMMA_FILESX86\Cisco\Cisco Secure Client\vpnagent.exe**
- **CSIDL_PROGRAM_FILESX86\Cisco\Cisco Secure Client\acnamlogonagent.exe**
- **CSIDL_PROGRAMMA_FILESX86\Cisco\Cisco Secure Client\acnamagent.exe**
- **CSIDL_PROGRAMMA_FILESX86\Cisco\Cisco Secure Client\UI\csc_ui.exe**
- **CSIDL_PROGRAM_FILES\Cisco\Secure Client\CM*\CMID*\csc_cmids.exe**
- **CSIDL_PROGRAM_FILES\Cisco\Secure Client\CM*\CMPM*\csc_pm.exe**
- **CSIDL_PROGRAM_FILES\Cisco\Secure Client\CM*\Service*\csc_cms.exe**
- **CSIDL_SYSTEM\appidpolicyconverter.exe**

Microsoft SQL Server

Uitgebreid tot V. 2019

toevoeging van:

- **CISCO_PROGRAM_FILES\Microsoft SQL Server*\MSSQL\Binn\SQLServr.exe**
- **CISCO_PROGRAM_FILES\Microsoft SQL Server*\OLAP\Bin\MSMDSrv.exe**
- **CSIDL_PROGRAM_FILES\Microsoft SQL Server*\Reporting Services\ReportServer\Bin\ReportingServicesService.exe**
- **CSIDL_PROGRAM_FILES\Microsoft SQL Server*\Shared\SQLDumper.exe**
- **CSIDL_PROGRAM_FILES\Microsoft SQL Server\MS***
- **CSIDL_PROGRAM_FILES\Microsoft SQL Server*\COM**
- **CSIDL_PROGRAM_FILES\Microsoft SQL Server*\DTS**
- **CSIDL_PROGRAM_FILES\Microsoft SQL Server*\Shared**

TrendMicro/Apex One

toevoeging van:

- CSIDL_PROGRAM_FILESX86\Trend Micro\Security Agent\CCSF\TMCCSF.exe
- CSIDL_PROGRAM_FILESX86\Trend Micro\Security Agent\TmPfw.exe
- CSIDL_PROGRAM_FILESX86\Trend Micro\Security Agent\TmListen.exe
- CSIDL_PROGRAM_FILESX86\Trend Micro\Security Agent\Ntrtscan.exe
- CISCO_PROGRAMMA_FILESX86\TREND Micro\iService\iATAS\ATASAgent.exe
- CISCO_PROGRAMMA_FILESX86\TREND Micro\iService\iAC\ac_bin\TMiACAgentSvc.exe
- CISCO_PROGRAMMA_FILESX86\TREND Micro\iService\iES\ESE\ESEServiceShell.exe
- CISCO_PROGRAMMA_FILESX86\TREND Micro\iService\iES\ESE\ESClient.exe
- CSIDL_PROGRAM_FILESX86\Trend Micro\BM\TMBMSRV.exe
- CSIDL_PROGRAM_FILESX86\Trend Micro\Security Agent\TMBMSRV.exe
- CISCO_PROGRAMMA_FILESX86\TREND Micro\iService\iVP\iVPAgent.exe
- CSIDL_PROGRAM_FILESX86\Trend Micro\Security Agent\TmSSClient.exe
- CSIDL_PROGRAM_FILESX86\Trend Micro\Security Agent\LogServer.exe
- CISCO_PROGRAMMA_FILESX86\TREND MICA\SECURITY Agent\Temp\LogServer\LogServer.exe
- CISCO_PROGRAMMA_FILESX86\TREND MICA\SECURITY Agent\CCSF\module\BES\TmsaInstance64.exe
- CSIDL_PROGRAM_FILESX86\Trend Micro\Security Agent\CNTAoSMgr.exe
- CSIDL_PROGRAM_FILESX86\Trend Micro\Security Agent\PccNTMon.exe
- CISCO_PROGRAMMA_FILESX86\TREND Micro\iService\iES\ESE\ESEFrameworkHost.exe
- CSIDL_SYSTEM\ShowMsg.exe
- CSIDL_SYSTEM\dsagent.exe
- .bkf

Nieuwe lijsten gemaakt

Azure DevOps - Windows

Oktober - 2022

Gedurende de maand oktober worden misvormde uitsluitingen die tijdens eerdere herhalingen van het product in de Secure Endpoint-omgeving zijn geïntroduceerd, uit de aangepaste uitsluitingslijsten verwijderd. Meer informatie over dit initiatief vindt u [hier](#).

14 december - 2022

Standaard Microsoft Windows

toevoeging van:

- C:\Windows\System32\omadmclient.exe
- .automatischeBestemmingen-ms

Veranderingen in backend - Windows

- **csc_ui.exe** toegevoegd aan Exploit Prevention Global Exclusions voor V5 en Script Control.

Verwijdering van: [Prestatie-invloedsuitsluitingen](#)

Nieuwe lijsten gemaakt

1Password - Windows, Mac, Linux

McAfee Trellix SolidCore - Windows

12 april - 2023

Standaard Microsoft Windows

toevoeging van:

- **.pf**
- **CSIDL_PROGRAMMA_FILESX86\Cisco\Cisco Secure Client\acumbrellagent.exe**

Verwijdering van:

- **CSIDL_WINDOWS\SoftwareDistribution\Datastore\Logs*.log**
- **CSIDL_SYSTEM\CatRoot2**
- **CSIDL_WINDOWS\Prefetch**

Microsoft Intune

toevoeging van:

- **CSIDL_PROGRAM_FILESX86\Microsoft Intune Management Extension\Microsoft.Management.Services.IntuneWindowsAgent.exe**

McAfee Trellix SolidCore

Kleine wijziging:

- **CSIDL_PROGRAM_FILESX86\McAfee\Policy Auditor Agent\engineMain.exe**

Cisco Webex

toevoeging van:

- **C:\Users*\AppData\WebEx\WebexHost.exe**

Microsoft Defender voor MacOS

toevoeging van:

- **/Library/Application Support/Microsoft/Defender/**

Microsoft Defender voor Linux

toevoeging van:

- **/opt/microsoft/mdatp/sbin/wdavdaemon**
- **/opt/microsoft/mdatp/**

31 mei - 2023

VEEAM

toevoeging van:

- **CSIDL_PROGRAM_FILES\Common Files\Veeam\Backup en replicatie\Explorers Recovery Service\Veeam.StandBy.Service.exe**
- **CSIDL_PROGRAM_FILES\Common Files\Veeam\Backup en replicatie\Mount Service\Veeam.Backup.MountService.exe**
- **CSIDL_PROGRAM_FILES\Veeam\Backup en replicatie\Veeam.Backup.BrokerService.exe**
- **CSIDL_PROGRAM_FILES\Veeam\Backup en replicatie\Veeam.Backup.CloudService.exe**
- **CSIDL_PROGRAM_FILES\Veeam\Backup en replicatie\Veeam.Backup.ExternalInfrastructure.DbProvider.exe**
- **CSIDL_PROGRAM_FILESX86\Veeam\Backup Transport\GuestInteraction\VSS\VeeamGuestHelperCtrl.exe**
- **CSIDL_PROGRAM_FILES\Veeam\Backup en replicatie\Backup\Veeam.Backup.Service.exe**
- **CSIDL_PROGRAM_FILES\Veeam\Backup en replicatie\Backup-catalogus\Veeam.Backup.CatalogDataService.exe**
- **CSIDL_PROGRAM_FILES\Veeam\Backup en replicatie\Backup\Veeam.Backup.ManagerGCServer.exe**
- **CSIDL_PROGRAM_FILES\Veeam\Backup en replicatie\Veeam.Backup.Cdp.Service.exe**
- **CSIDL_PROGRAM_FILES\Veeam\Backup en replicatie\Console\veam.backup.shell.exe**
- **CSIDL_PROGRAM_FILESX86\Veeam\Backup Transport\x64\VeeamAgent.exe**
- **CSIDL_PROGRAM_FILES\Veeam\Backup en replicatie\Backup\Veeam.Backup.Manager.exe**
- **CSIDL_WINDOWS\Veeam\Backup\VeeamDeploymentSvc.exe**
- **.vbm.temp**
- **.flat**

VMWare

toevoeging van:

- **CSIDL_PROGRAM_FILES\Common Files\VMware\ScannerRedirection\ftscanmgrhv.exe**
- **CSIDL_PROGRAM_FILESX86\VMware\VMware Horizon View Client\ClientService\horizon_client_service.exe**

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.