

思科維護的思科安全端點控制檯的排除清單更改

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[更新時的預期](#)

[變更](#)

[2019年8月28日](#)

[Microsoft Windows預設值：](#)

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

[Docker - Mac:](#)

[已建立的新清單：](#)

[9月18日 — 2019年](#)

[Apple MacOS預設值：](#)

[McAfee - Mac](#)

[Cisco Jabber - Mac](#)

[Crashplan - Mac](#)

[JAMF Casper - Mac](#)

[VMWare Fusion - Mac](#)

[Xcode - Mac](#)

[一個驅動器 — Windows](#)

[Citrix ICA客戶端 — Windows](#)

[已建立的新清單：](#)

[12月11日 — 2019年](#)

[一個驅動器 — Windows](#)

[Splunk - Windows](#)

[Splunk - Linux](#)

[已建立的新清單：](#)

[2020年2月12日](#)

[Microsoft Windows預設值 — Windows](#)

[Websense - Windows](#)

[Microsoft SQL Server - Windows](#)

[2020年6月10日](#)

[Malwarebytes - Windows](#)

[Microsoft Office - Windows](#)

[IIS - Windows](#)

[Altiris by Symantec - Windows](#)

[McAfee - Windows](#)

[已建立的新清單：](#)

[7月15日 — 2020年](#)

[域控制器 — Windows](#)

[Microsoft Teams - Windows](#)

[已建立新清單](#)

[8月26日 — 2020年](#)

[Microsoft SQL Server - Windows](#)

[9月30日 — 2020年](#)

[Malwarebytes - Windows](#)

[數位監護人 — Mac](#)

[已建立新清單](#)

[3月3日 — 2021年](#)

[卡巴斯基 — Windows](#)

[SCCM - Windows](#)

[Symantec - Windows](#)

[已建立新清單](#)

[2021年6月30日](#)

[Microsoft Windows預設值](#)

[Citrix ICA客戶端](#)

[Citrix Provisioning Server](#)

[已建立新清單](#)

[9月29日 — 2021年](#)

[Cisco Webex - Windows](#)

[Crashplan - Windows](#)

[Crashplan - Mac](#)

[VMware - Windows](#)

[3月23日 — 2022年](#)

[Microsoft Windows預設值](#)

[Hyper-V - Windows](#)

[Microsoft Windows Defender - Windows](#)

[6月29日 — 2022年](#)

[Microsoft Windows預設值](#)

[Cisco AnyConnect VPN](#)

[Cisco Webex](#)

[Microsoft OneDrive \(以前是一個驅動器\)](#)

[Tanium - Windows](#)

[Citrix Provisioning Server](#)

[已建立新清單](#)

[9月14日 — 2022年](#)

[Microsoft Windows預設值](#)

[Microsoft SQL Server](#)

[趨勢科技/Apex One](#)

[已建立新清單](#)

[2022年10月](#)

[12月14日 — 2022年](#)

[Microsoft Windows預設值](#)

[後端更改 — Windows](#)

[已建立新清單](#)

[4月12日 — 2023年](#)

[Microsoft Windows預設值](#)

[Microsoft Intune](#)

[McAfee Trellix SolidCore](#)

[Cisco Webex](#)

[Microsoft Defender for MacOS](#)

[Microsoft Defender for Linux](#)

[5月31日 — 2023年](#)

[VEEAM](#)

[VMWare](#)

[9月27日 — 2023年](#)

[Cisco Webex](#)

[Microsoft OneNote](#)

[Microsoft SQL Server](#)

[Microsoft Team](#)

[Microsoft Windows預設值](#)

[斯普倫克](#)

[Symantec Endpoint Protection](#)

[已建立新清單](#)

[11月22日–2023年](#)

[Microsoft Windows預設值](#)

[Citrix ICA客戶端](#)

[已建立新清單](#)

[1月24日 — 2024年](#)

[已建立新清單](#)

簡介

本檔案介紹新增至思科維護的例外專案的變更。

思科維護的例外項由思科建立並維護，以便在面向終端聯結器的高級惡意軟體防護(AMP)與防病毒、安全或其他軟體之間提供更好的相容性，這些例外項可新增到應用程式的新版本中。

必要條件

需求

思科建議您瞭解以下主題：

- 面向終端的AMP中的排除項
- AMP 主控台

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- AMP端點版控制台5.4.20190820

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。

更新時的預期

Exclusions

Show Custom Exclusions Cisco-Maintained Exclusions ?

Search by exclusion set, path, extension, threat name, or SHA-256

All Products Windows Mac Linux

Cisco-Maintained Exclusions are created and maintained by Cisco to provide better compatibility between the AMP for Endpoints Connector and antivirus, security, or other software. These exclusions may be updated with improvements and new exclusions may be added for new versions of an application.

更改思科維護的清單後，將在後端進行策略更新以反映該更改。當每個端點在其心跳中使用該清單簽入時，它們會提取更新的策略。這些策略更改不會反映在稽核日誌中，因為從技術上講，這是對排除清單的更改，而不是策略本身，並且思科維護的排除清單不存在於單個控制檯上的正常稽核日誌中。對於大規模環境，這看起來像是大量策略更新，最終結果將是每個端點獲得更好的效能。

更新週期取決於每個端點。如果所有機器都線上，更新將在1-2個心跳內發生。如果是在全球環境下，電腦聯機時會繼續進行更新，因此，在推送維護的清單後的24-48小時內，不要驚訝地看到其他策略更新。

變更

2019年8月28日

Microsoft Windows預設值：

刪除：

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

原因：重復性。基集中的另一個排除項覆蓋了它。

新增：

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

原因：由於進程掃描，Windows 10更新偶爾失敗。

N-Able Solar Winds - Windows:

新增：

- C:\Program 檔案(x86)\N-able Technologies\Windows Agent\bin\agent.exe
- C:\Program 檔案(x86)\BeAnywhere 支援Express\GetSupportService_N-Central\BASupSvc.exe
- C:\Program 檔案(x86)\N-able Technologies\PatchManagement\ThirdPartyPatch\ThirdPartyPatch.exe

Docker - Mac:

刪除：

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

原因: 額外的測試讓我們對安全性產生了擔憂，因此開發工作已經精確定位了更好的例外情況。

新增：

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

已建立的新清單：

Linux:

- Docker — 聯結器1.10.2
- Docker — 聯結器1.11+
- 扎比克斯

Mac:

- 虛擬盒
- 數位監護人

9月18日 — 2019年

Apple MacOS預設值：

新增：

- /Applications/Time Machine.app/Contents/MacOS/Time Machine
- /System/Library/CoreServices/Spotlight.app/Contents/MacOS/Spotlight

McAfee - Mac

新增：

- /Library/McAfee/Agent/bin/CmdAgent

Cisco Jabber - Mac

刪除：

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

原因：安全性更高，基於流程的排除功能更豐富。

新增：

- /Applications/Cisco Jabber.app/Contents/MacOS/Cisco Jabber

Crashplan - Mac

新增：

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

JAMF Casper - Mac

刪除：

- /usr/bin/sw_vers

原因：安全性更高，基於流程的排除功能更豐富。

新增：

- /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

新增：

- /Applications/VMware Fusion.app/Contents/MacOS/VMware Fusion

Xcode - Mac

新增：

- /Applications/Xcode.app/Contents/SharedFrameworks/XCBuild.framework/Versions/A/PlugIns/XCBuildService.bundle/Co
- /Applications/Xcode.app/Contents/Developer/usr/bin/xcodebuild

一個驅動器 — Windows

細微更改：

- C:*Users\OneDrive\ (添加反斜線以提高安全性)

Citrix ICA客戶端 — Windows

新增：

- 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

原因：最近更新了Citrix建議的排除項。

已建立的新清單：

Windows

- Citrix Provisioning Server
- Citrix雲端連結器

12月11日 — 2019年

一個驅動器 — Windows

新增：

- CSIDL_LOCAL_APPDATA\Microsoft\OneDrive\OneDrive.exe

Splunk - Windows

新增：

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

Splunk - Linux

新增：

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

已建立的新清單：

Azure - Linux

Vagrant - Mac

2020年2月12日

Microsoft Windows預設值 — Windows

新增：

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

Websense - Windows

新增：

- [多個驅動器]:\Program Files*\Websense\
 - C:\Program 檔案(x86)\Websense\Websense Endpoint\dserui.exe
 - C:\Program Files\Websense\Websense Endpoint\dserui.exe
 - C:\Program 檔案(x86)\Websense\Websense Endpoint\EndPointClassifier.exe
 - C:\Program 檔案(x86)\Websense\Websense Endpoint\FILTERSDK\kvoop.exe
 - C:\Program 檔案(x86)\Websense\Websense Endpoint\wepsvc.exe

Microsoft SQL Server - Windows

新增：

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

2020年6月10日

Malwarebytes - Windows

細微更改：

- C:\ProgramData\Malwarebytes端點代理\
 - C:\ProgramData\Malwarebytes\MBAMService\
 - .sql

Microsoft Office - Windows

新增：

- C:\Program Files\Common Files\microsoft shared\ClickToRun\OfficeClickToRun.exe

IIS - Windows

新增：

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

Altiris by Symantec - Windows

新增：

- C:\Program Files\Altiris\Altiris代理\AeXNSAgent.exe

McAfee - Windows

新增：

- C:\Program Files\McAfee\Endpoint安全\自適應威脅防護\mfeatp.exe

已建立的新清單：

NetScout - Windows

IBM - Windows

7月15日 — 2020年

域控制器 — Windows

新增：

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

Microsoft Teams - Windows

新增：

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

已建立新清單

控制啟動

8月26日 — 2020年

**由於進行其他測試，原發行日期從19日延長到26日

Microsoft SQL Server - Windows

正在替換：

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

新增：

- CSIDL_PROGRAM_FILES\Microsoft SQL Server\MSSQL.11\MSSQL\Binn\SQLServr.exe
- CSIDL_PROGRAM_FILES\Microsoft SQL Server\MSSQL.12\MSSQL\Binn\SQLServr.exe
- CSIDL_PROGRAM_FILES\Microsoft SQL Server\MSSQL.13\MSSQL\Binn\SQLServr.exe
- CSIDL_PROGRAM_FILES\Microsoft SQL Server\MSSQL.11\OLAP\Bin\MSMDSrv.exe
- CSIDL_PROGRAM_FILES\Microsoft SQL Server\MSSQL.12\OLAP\Bin\MSMDSrv.exe
- CSIDL_PROGRAM_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

9月30日 — 2020年

Malwarebytes - Windows

新增：

- CSIDL_PROGRAM_FILES\Malwarebytes' Anti-Malware\mbam.exe
- CSIDL_PROGRAM_FILESX86\Malwarebytes' Anti-Malware\mbam.exe

數位監護人 — Mac

新增：

- /usr/local/dgagent
- /dgagent

已建立新清單

數位監護人 — Windows

3月3日 — 2021年

卡巴斯基 — Windows

新增：

- CSIDL_PROGRAM_FILESX86\Kaspersky Lab\Kaspersky Endpoint Security for Windows\avp.exe
- CSIDL_PROGRAM_FILESX86\卡巴斯基實驗室\網路代理\klnagent.exe

SCCM - Windows

刪除：

- WINDOWS\CCM\ServiceData -重複路徑

- Program Files\Microsoft Configuration Manager\EasySetupPayload -重複路徑

Symantec - Windows

新增：

- 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\12.1.6608.6300.105\Bin\ccSvcHst.exe
- CSIDL_PROGRAM_FILESX86\Symantec\Symantec Endpoint Protection\12.1.7061.6600.105\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

已建立新清單

Cisco AnyConnect - Windows

Microsoft Defender ATP - Windows

2021年6月30日

Microsoft Windows預設值

新增：

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

Citrix ICA客戶端

新增：

- 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客戶端\

Citrix Provisioning Server

刪除：

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

新增：

- 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

已建立新清單

Commvault - Windows

Citrix Sessions Recording - Windows

9月29日 — 2021年

Cisco Webex - Windows

新增：

- 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

新增：

- CSIDL_PROGRAM_FILES\Code42\Code42Service.exe

Crashplan - Mac

新增：

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

VMware - Windows

新增：

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

3月23日 — 2022年

Microsoft Windows預設值

新增：

- C:\Windows\System32\SearchIndexer.exe

Hyper-V - Windows

新增：

- CSIDL_COMMON_APPDATA\Microsoft\Windows\Hyper-V\
- CSIDL_COMMON_DOCUMENTS\Hyper-V\虛擬硬碟\

Microsoft Windows Defender - Windows

新增：

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

6月29日 — 2022年

Microsoft Windows預設值

新增：

- *.applocker

Cisco AnyConnect VPN

新增：

- CSIDL_PROGRAM_FILESX86\Cisco\Cisco AnyConnect安全移動客戶端\acwebhelper.exe

Cisco Webex

新增：

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

Microsoft OneDrive (以前是一個驅動器)

新增：

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

Tanium - Windows

新增：

- C:\Program檔案(x86)\Tanium\Tanium終端使用者通知工具\bin\end-user-notifications.exe

Citrix Provisioning Server

新增：

- CSIDL_PROGRAM_FILES\Citrix\Provisioning Services\MgmtDaemon.com

刪除：

- CSIDL_PROGRAM_FILES\Citrix\Provisioning Services\MgmtDaemon.com

已建立新清單

X1搜尋 — Windows

Microsoft Intune - Windows

9月14日 — 2022年

Microsoft Windows預設值

新增：

- CSIDL_PROGRAM_FILESX86\Cisco\Cisco安全客戶端\
- CSIDL_PROGRAM_FILESX86\Cisco\Cisco Secure Client\UI\acumbrellaagent.exe
- CSIDL_PROGRAM_FILESX86\Cisco\Cisco Secure Client\UI\acumbrellaagent.exencrypt-proxy.exe
- CSIDL_PROGRAM_FILESX86\Cisco\Cisco Secure Client\NVM\acnvmagent.exe
- CSIDL_PROGRAM_FILESX86\Cisco\Cisco安全客戶端\vpnagent.exe
- CSIDL_PROGRAM_FILESX86\Cisco\Cisco安全客戶端\acnamlogonagent.exe
- CSIDL_PROGRAM_FILESX86\Cisco\Cisco Secure Client\acnamagent.exe
- CSIDL_PROGRAM_FILESX86\Cisco\Cisco Secure Client\UI\csc_ui.exe
- CSIDL_PROGRAM_FILES\Cisco\Cisco Secure Client\CM*\CMID*\csc_cmids.exe
- CSIDL_PROGRAM_FILES\Cisco\Cisco Secure Client\CM*\CMPM*\csc_pm.exe
- CSIDL_PROGRAM_FILES\Cisco\Cisco Secure Client\CM*\Service*\csc_cms.exe
- CSIDL_SYSTEM\appidpolicyconverter.exe

Microsoft SQL Server

擴展至包括V. 2019

新增：

- CSIDL_PROGRAM_FILES\Microsoft SQL Server*\MSSQL\Binn\SQLServr.exe
- CSIDL_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\

趨勢科技/Apex One

新增：

- CSIDL_PROGRAM_FILESX86\Trend Micro\Security Agent\CCSF\TMCCSF.exe
- CSIDL_PROGRAM_FILESX86\Trend Micro\Security Agent\TmPfw.exe
- CSIDL_PROGRAM_FILESX86\趨勢科技\安全代理\TmListen.exe
- CSIDL_PROGRAM_FILESX86\Trend Micro\Security Agent\Ntrtscan.exe
- CSIDL_PROGRAM_FILESX86\Trend Micro\iService\iATAS\ATASAgent.exe
- CSIDL_PROGRAM_FILESX86\Trend Micro\iService\iAC\ac_bin\TMiACAgentSvc.exe
- CSIDL_PROGRAM_FILESX86\Trend Micro\iService\iES\ESE\ESEServiceShell.exe
- CSIDL_PROGRAM_FILESX86\Trend Micro\iService\iES\ESE\ESEClient.exe
- CSIDL_PROGRAM_FILESX86\Trend Micro\BM\TMBMSRV.exe
- CSIDL_PROGRAM_FILESX86\Trend Micro\Security Agent\TMBMSRV.exe
- CSIDL_PROGRAM_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
- CSIDL_PROGRAM_FILESX86\Trend Micro\Security Agent\Temp\LogServer\LogServer.exe
- CSIDL_PROGRAM_FILESX86\Trend Micro\Security Agent\CCSF\module\BES\TmsalInstance64.exe
- CSIDL_PROGRAM_FILESX86\Trend Micro\Security Agent\CNTAoSMgr.exe
- CSIDL_PROGRAM_FILESX86\Trend Micro\Security Agent\PccNTMon.exe
- CSIDL_PROGRAM_FILESX86\Trend Micro\iService\iES\ESE\ESEFrameworkHost.exe
- CSIDL_SYSTEM\ShowMsg.exe
- CSIDL_SYSTEM\dsagent.exe
- .bkf

已建立新清單

Azure DevOps - Windows

2022年10月

在10月份，將在產品早期迭代期間引入到安全終端環境的格式不正確的排除項將從自定義排除清單中刪除。可在此處找到有關此計畫的更多[資訊](#)。

12月14日 — 2022年

Microsoft Windows預設值

新增：

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

後端更改 — Windows

- csc_ui.exe 已新增到V5和指令碼控制的漏洞防護全域性排除。

刪除：影響[效能的排除](#)

已建立新清單

1密碼 — Windows、Mac、Linux

McAfee Trellix SolidCore - Windows

4月12日 — 2023年

Microsoft Windows預設值

新增：

- .pf
- CSIDL_PROGRAM_FILESX86\Cisco\Cisco安全客戶端\acumbrellaagent.exe

刪除：

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

Microsoft Intune

新增：

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

McAfee Trellix SolidCore

細微更改：

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

Cisco Webex

新增：

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

Microsoft Defender for MacOS

新增：

- /Library/Application Support/Microsoft/Defender/

Microsoft Defender for Linux

新增：

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

5月31日 — 2023年

VEEAM

新增：

- CSIDL_PROGRAM_FILES\Common Files\Veeam\Backup and Replication\Explorer Recovery Service\Veeam.Standby.Service.exe
- CSIDL_PROGRAM_FILES\Common Files\Veeam\Backup and Replication\Mount Service\Veeam.Backup.MountService.exe
- CSIDL_PROGRAM_FILES\Veeam\Backup and Replication\Backup\Veeam.Backup.BrokerService.exe
- CSIDL_PROGRAM_FILES\Veeam\Backup and Replication\Backup\Veeam.Backup.CloudService.exe
- CSIDL_PROGRAM_FILES\Veeam\Backup and Replication\Backup\Veeam.Backup.ExternalInfrastructure.DbProvider.exe
- CSIDL_PROGRAM_FILESX86\Veeam\Backup Transport\GuestInteraction\VSS\VeeamGuestHelperCtrl.exe
- CSIDL_PROGRAM_FILES\Veeam\Backup and Replication\Backup\Veeam.Backup.Service.exe
- CSIDL_PROGRAM_FILES\Veeam\Backup and Replication\Backup Catalog\Veeam.Backup.CatalogDataService.exe
- CSIDL_PROGRAM_FILES\Veeam\Backup and Replication\Backup\Veeam.Backup.ManagerGCServer.exe
- CSIDL_PROGRAM_FILES\Veeam\Backup and Replication\Backup\Veeam.Backup.Cdp.Service.exe
- CSIDL_PROGRAM_FILES\Veeam\Backup and Replication\Console\veeam.backup.shell.exe
- CSIDL_PROGRAM_FILESX86\Veeam\Backup Transport\x64\VeeamAgent.exe

- CSIDL_PROGRAM_FILES\Veeam\Backup and Replication\Backup\Veeam.Backup.Manager.exe
- CSIDL_WINDOWS\Veeam\Backup\VeeamDeploymentSvc.exe
- .vbm.temp
- .flat

VMWare

新增：

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

9月27日 — 2023年

Cisco Webex

新增：

- CSIDL_LOCAL_APPDATA\Programs\Cisco Spark\CiscoCollabHost.exe

Microsoft OneNote

新增：

- CSIDL_LOCAL_APPDATA\Microsoft\OneNote*\cache*.bin

Microsoft SQL Server

新增：

- CSIDL_PROGRAM_FILES\Microsoft SQL Server*\MSSQL\Binn\sqlagent.exe
- CSIDL_PROGRAM_FILES\Microsoft SQL Server*\MSSQL\Binn\MsDtsSrvr.exe
- CSIDL_PROGRAM_FILES\Microsoft SQL Server*\Shared\sqlbrowser.exe
- CSIDL_WINDOW\Cluster\
- CSIDL_PROGRAM_FILES\Microsoft SQL Server*\MSSQL\FTDATA\
- CSIDL_WINDOW\Cluster\clussvc.exe
- CSIDL_WINDOW\Cluster\rhs.exe
- .trc

删除：

- CSIDL_PROGRAM_FILES\Microsoft SQL Server\MSSQL.11\MSSQL\Binn\SQLServr.exe
- CSIDL_PROGRAM_FILES\Microsoft SQL Server\MSSQL.11\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\MSSQL\Binn\SQLServr.exe
- CSIDL_PROGRAM_FILES\Microsoft SQL Server\MSSQL.12\OLAP\Bin\MSMDSrv.exe
- CSIDL_PROGRAM_FILES\Microsoft SQL Server\MSSQL.12\Reporting Services\ReportServer\Bin\ReportingServicesService.exe
- CSIDL_PROGRAM_FILES\Microsoft SQL Server\MSSQL.13\MSSQL\Binn\SQLServr.exe
- CSIDL_PROGRAM_FILES\Microsoft SQL Server\MSSQL.13\OLAP\Bin\MSMDSrv.exe
- CSIDL_PROGRAM_FILES\Microsoft SQL Server\MSSQL.13\Reporting Services\ReportServer\Bin\ReportingServicesService.exe
- CSIDL_PROGRAM_FILES\Microsoft SQL Server\MSSQL*.MSSQLSERVER\MSSQL\Binn\SQLServr.exe
- CSIDL_PROGRAM_FILES\Microsoft SQL Server\MSAS*.MSSQLSERVER\OLAP\Bin\MSMDSrv.exe
- CSIDL_PROGRAM_FILES\Microsoft SQL Server\MSRS*.MSSQLSERVER\Reporting Services\ReportServer\Bin\ReportingServicesService.exe
- .abf
- .ctl
- .dbf
- .rdo

Microsoft Team

新增：

- CSIDL_LOCAL_APPDATA\Microsoft\Teams\current\squirrel.exe
- CSIDL_LOCAL_APPDATA\Microsoft\TeamsMeetingAddin

Microsoft Windows 預設值

新增：

- CSIDL_WINDOWS\WinSxS*\TiWorker.exe

斯普倫克

新增：

- CSIDL_PROGRAM_FILES\splunk\bin\splunk.exe
- CSIDL_PROGRAM_FILES\splunk\bin\splunk*.exe

Symantec Endpoint Protection

新增：

- CSIDL_PROGRAM_FILES\Symantec\Symantec Endpoint Protection*\Bin64\ccSvcHst.exe
- CSIDL_COMMON_APPDATA\Symantec\Symantec Endpoint Protection\
- CSIDL_PROGRAM_FILESX86\Symantec\Symantec Endpoint Protection*\Bin64\Smc.exe

刪除：

- CSIDL_WINDOWS\Temp\TMP*.tmp
- CSIDL_WINDOWS\Temp\musdmys_*
- CSIDL_WINDOWS\Temp\content.zip.tmp\SymDeltaDecompressOptions.xml
- CSIDL_WINDOWS\Temp\content.zip.tmp*.diff
- CSIDL_WINDOWS\Temp\content.zip.tmp\cur.scr
- CSIDL_COMMON_APPDATA\Symantec\

已建立新清單

- Zscaler使用者端連結器
- ManageEngine端點中心
- Symantec資料丟失保護

11月22日–2023年

Microsoft Windows預設值

新增：

- CSIDL_PROGRAM_FILES\Cisco\Orbital\python\python.exe

Citrix ICA客戶端

新增：

- CSIDL_PROGRAM_FILESEX86\Citrix\ICA Client\SelfServicePlugin\SelfService.exe
- CSIDL_PROGRAM_FILESEX86\Citrix\ICA Client\SelfServicePlugin\SelfServicePlugin.exe
- CSIDL_PROGRAM_FILESEX86\Citrix\ICA Client\Receiver\FeatureFlag\CWAFeatureFlagUpdater.exe
- CSIDL_PROGRAM_FILESEX86\Citrix\ICA Client\wfcrun32.exe
- CSIDL_PROGRAM_FILESEX86\Citrix\ICA Client\Receiver\Receiver.exe

已建立新清單

- Ivanti LANDesk
- Atera代理

1月24日 — 2024年

Microsoft SQL Server和Azure DevOps需要與Windows終結點8.2.1+的排除處理更改相關的次要調整。未新增任何排除。

已建立新清單

- 北極狼

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）。