Cambios en la lista de exclusión mantenida por Cisco para Cisco Secure Endpoint Console

Contenido

Del 15 de julio al 2020
Controladores de dominio - Windows
Microsoft Teams - Windows
Nueva lista creada
Del 26 de agosto al 2020
Microsoft SQL Server - Windows
Del 30 de septiembre al 2020
Malwarebytes: Windows
Digital Guardian (Mac)
Nueva lista creada
3 de marzo - 2021
Kaspersky - Windows
SCCM - Windows
Symantec (Windows)
Nuevas listas creadas
Del 30 de junio al 2021
Predeterminado de Microsoft Windows
Cliente ICA de Citrix
Citrix Provisioning Server
Nuevas listas creadas
Del 29 de septiembre al 2021
Cisco Webex: Windows
Crashplan - Windows
Crashplan para Mac
VMware - Windows
Del 23 de marzo al 2022
Predeterminado de Microsoft Windows
Hyper-V: Windows
Microsoft Windows Defender: Windows
Del 29 de junio al 2022
Predeterminado de Microsoft Windows
VPN Cisco AnyConnect
Cisco Webex
Microsoft OneDrive (anteriormente One Drive)
Tanio - Ventanas
Citrix Provisioning Server
Nuevas listas creadas
Del 14 de septiembre al 2022
Predeterminado de Microsoft Windows
Microsoft SQL Server
TrendMicro y Apex One
Nuevas listas creadas
Octubre - 2022
Del 14 de diciembre al 2022
Predeterminado de Microsoft Windows
Cambios en el motor: Windows
Nuevas listas creadas

Introducción

Este documento describe los cambios agregados a las exclusiones mantenidas por Cisco.

Cisco crea y mantiene las exclusiones mantenidas por Cisco para proporcionar una mejor compatibilidad entre la protección frente a malware avanzado (AMP) para el conector de terminales y el antivirus, la seguridad u otro software. Estas exclusiones se pueden agregar a nuevas versiones de una aplicación.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Exclusiones de AMP para terminales
- consola AMP

Componentes Utilizados

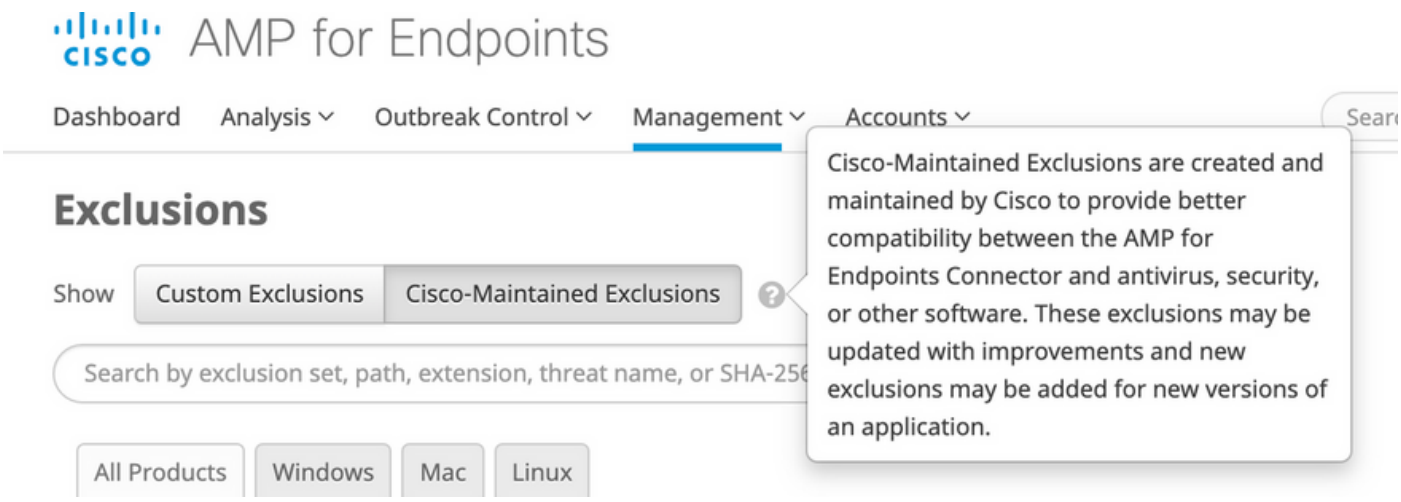
La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- AMP para terminales, versión de consola 5.4.20190820

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en

funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Expectativas al actualizar



Cuando se cambian las listas de mantenimiento de Cisco, se produce una actualización de la política en el back-end para reflejar ese cambio. A medida que cada uno de los terminales utiliza esa lista para protegerse en sus latidos, extraen la política actualizada. Estos cambios de políticas no se reflejan en el registro de auditoría, ya que técnicamente se trata de un cambio en la lista de exclusión, no en la política en sí, y las listas de exclusión mantenidas por Cisco no existen dentro del registro de auditoría normal en las consolas individuales. En entornos de gran escala, parece una avalancha de actualizaciones de políticas y el resultado final será un mejor rendimiento en cada uno de los terminales.

El período de actualización depende de cada punto final. Si todas las máquinas están en línea, las actualizaciones tendrían lugar dentro de 1-2 latidos. Si se trata de un entorno global, las actualizaciones continúan produciéndose a medida que los equipos se conectan, por lo que no se sorprenda al ver actualizaciones de políticas adicionales 24-48 horas después de que se envíe la lista de mantenimiento.

Cambios

Del 28 de agosto al 2019

Predeterminado de Microsoft Windows:

Eliminación de:

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

Motivo: Repetitivo. Otra exclusión en el conjunto base lo cubre.

Adición de:

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

Motivo: las actualizaciones de Windows 10 fallaron esporádicamente debido a los análisis de los procesos.

N-Able Vientos Solares - Ventanas:

Adición de:

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

Docker para Mac:

Eliminación de:

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

Motivo: Una prueba adicional nos ha dejado preocupados por la seguridad, por lo que el desarrollo ha identificado mejores exclusiones.

Adición de:

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

Nuevas listas creadas:

Linux:

- Acoplador - Conector 1.10.2
- Acoplador - Conector 1.11+
- Zabbix

Mac:

- Caja virtual
- Guardián digital

18 de septiembre - 2019

Apple MacOS predeterminado:

Adición de:

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

McAfee - Mac

Adición de:

- /Library/McAfee/Agent/bin/CmdAgent

Cisco Jabber para Mac

Eliminación de:

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

Motivo: mayor seguridad y funcionalidad adicional de las exclusiones basadas en procesos.

Adición de:

- **/Aplicaciones/Cisco Jabber.app/Contents/MacOS/Cisco Jabber**

Crashplan para Mac

Adición de:

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

JAMF Casper (Mac)

Eliminación de:

- /usr/bin/sw_vers

Motivo: mayor seguridad y funcionalidad adicional de las exclusiones basadas en procesos.

Adición de:

- /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 para Mac

Adición de:

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

Xcode para Mac

Adición de:

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

Una unidad: Windows

Cambio menor:

- C:*\Users\OneDrive\ (se ha añadido la barra diagonal inversa para mejorar la seguridad)

Citrix Cliente ICA - Windows

Adición de:

- 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

Motivo: actualización reciente de exclusiones sugeridas por Citrix.

Nuevas listas creadas:

Windows:

- Citrix Provisioning Server
- Conector de nube de Citrix

Del 11 de diciembre al 2019

Una unidad: Windows

Adición de:

- CSIDL_LOCAL_APPDATA\Microsoft\OneDrive\OneDrive.exe

Splunk: Windows

Adición de:

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

Splunk - Linux

Adición de:

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

Nuevas listas creadas:

Azure - Linux

Vagrant - Mac

Del 12 de febrero al 2020

Predeterminado de Microsoft Windows: Windows

Adición de:

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

Websense: Windows

Adición de:

- [Varias Unidades]:\Archivos De Programa*\Websense\
- C:\Program Files (x86)\Websense\Websense Endpoint\dserui.exe
- C:\Program Files\Websense\Websense Endpoint\dserui.exe
- C:\Program Files (x86)\Websense\Websense Endpoint\EndPointClassifier.exe
- C:\Program Files (x86)\Websense\Websense Endpoint\FilterSDK\kvoop.exe
- C:\Program Files (x86)\Websense\Websense Endpoint\wepsvc.exe

Microsoft SQL Server - Windows

Adición de:

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

Del 10 de junio al 2020

Malwarebytes: Windows

Cambio menor:

- C:\ProgramData\Malwarebytes Agente de terminales\
- C:\ProgramData\Malwarebytes\MBAMService\

Microsoft Office - Windows

Adición de:

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

IIS: Windows

Adición de:

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

Altiris by Symantec (Windows)

Adición de:

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

McAfee - Windows

Adición de:

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

Nuevas listas creadas:

NetScout para Windows

IBM: Windows

Del 15 de julio al 2020

Controladores de dominio - Windows

Adición de:

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

Microsoft Teams - Windows

Adición de:

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

Nueva lista creada

Control activado

Del 26 de agosto al 2020

**Debido a pruebas adicionales, la fecha de lanzamiento original se amplió del 19 al 26

Microsoft SQL Server - Windows

Sustitución:

- 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

Adición de:

- 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

Del 30 de septiembre al 2020

Malwarebytes: Windows

Adición de:

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

Digital Guardian (Mac)

Adición de:

- /usr/local/dgagent
- /dgagent

Nueva lista creada

Guardián digital: Windows

3 de marzo - 2021

Kaspersky - Windows

Adición de:

- CSIDL_PROGRAM_FILESX86\Kaspersky Lab\Kaspersky Endpoint Security for Windows\avp.exe
- CSIDL_PROGRAM_FILESX86\Kaspersky Lab\NetworkAgent\klnagent.exe

SCCM - Windows

Eliminación de:

- WINDOWS\CCM\ServiceData - Ruta duplicada
- Archivos de programa\Microsoft Configuration Manager\EasySetupPayload - Ruta duplicada

Symantec (Windows)

Adición de:

- 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

Nuevas listas creadas

Cisco AnyConnect (Windows)

ATP de Microsoft Defender: Windows

Del 30 de junio al 2021

Predeterminado de Microsoft Windows

Adición de:

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

Cliente ICA de Citrix

Adición de:

- 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

Eliminación de:

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

Adición de:

- 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\MgmntDaemon.exe
- CSIDL_PROGRAM_FILES\Citrix\Provisioning Services\BNPXE.exe
- CSIDL_PROGRAM_FILES\Citrix\Provisioning Services\BNDevice.exe

Nuevas listas creadas

Commvault - Windows

Grabación de sesiones de Citrix: Windows

Del 29 de septiembre al 2021

Cisco Webex: Windows

Adición de:

- 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

Adición de:

- CSIDL_PROGRAM_FILES\Code42\Code42Service.exe

Crashplan para Mac

Adición de:

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

VMware - Windows

Adición de:

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

Del 23 de marzo al 2022

Predeterminado de Microsoft Windows

Adición de:

- C:\Windows\System32\SearchIndexer.exe

Hyper-V: Windows

Adición de:

- CSIDL_COMMON_APPDATA\Microsoft\Windows\Hyper-V\
- CSIDL_COMMON_DOCUMENTS\Hyper-V\Discos duros virtuales\

Microsoft Windows Defender: Windows

Adición de:

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

Del 29 de junio al 2022

Predeterminado de Microsoft Windows

Adición de:

- *.applocker

VPN Cisco AnyConnect

Adición de:

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

Cisco Webex

Adición de:

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

Microsoft OneDrive (anteriormente One Drive)

Adición de:

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

Tanio - Ventanas

Adición de:

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

Citrix Provisioning Server

Adición de:

- CSIDL_PROGRAM_FILES\Citrix\Provisioning Services\MgmtDaemon.com

Eliminación de:

- CSIDL_PROGRAM_FILES\Citrix\Provisioning Services\MgmntDaemon.com

Nuevas listas creadas

Búsqueda X1 - Windows

Microsoft Intune - Windows

Del 14 de septiembre al 2022

Predeterminado de Microsoft Windows

Adición de:

- CSIDL_PROGRAM_FILESX86\Cisco\Cisco Secure Client\
- CSIDL_PROGRAM_FILESX86\Cisco\Cisco Secure Client\UI\acumbrellaagent.exe

- CSIDL_PROGRAM_FILESX86\Cisco\Cisco Secure Client\UI\acumbrellaagent.exenscrypt-proxy.exe
- CSIDL_PROGRAM_FILESX86\Cisco\Cisco Secure Client\NVM\acnvmagent.exe
- CSIDL_PROGRAM_FILESX86\Cisco\Cisco Secure Client\vpnagent.exe
- CSIDL_PROGRAM_FILESX86\Cisco\Cisco Secure Client\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_cmid.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

Ampliado para incluir V. 2019

Adición de:

- 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\

TrendMicro y Apex One

Adición De:

- 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
- 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\ESClient.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\TmsaInstance64.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

Nuevas listas creadas

Azure DevOps - Windows

Octubre - 2022

Durante el mes de octubre, las exclusiones incorrectas que se introdujeron en el entorno de terminales seguros durante iteraciones anteriores del producto se eliminarán de las listas de exclusión personalizadas. Más información relacionada con esta iniciativa se puede encontrar aquí.

Del 14 de diciembre al 2022

Predeterminado de Microsoft Windows

Adición de:

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

Cambios en el motor: Windows

- csc_ui.exe agregado a Exclusiones globales de prevención de vulnerabilidades para V5 y control de scripts.

Eliminación de: Exclusiones que afectan al rendimiento

Nuevas listas creadas

1Contraseña: Windows, Mac, Linux

McAfee Trellix SolidCore - Windows

Del 12 de abril al 2023

Predeterminado de Microsoft Windows

Adición de:

- .pf
- CSIDL_PROGRAM_FILESX86\Cisco\Cisco Secure Client\acumbrellaagent.exe

Eliminación de:

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

Microsoft Intune

Adición de:

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

McAfee Trellix SolidCore

Cambio menor:

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

Cisco Webex

Adición de:

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

Microsoft Defender para MacOS

Adición de:

- /Library/Application Support/Microsoft/Defender/

Microsoft Defender para Linux

Adición de:

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

31 de mayo - 2023

VEEAM

Adición de:

- CSIDL_PROGRAM_FILES\Common Files\Veeam\Backup and Replication\Explorers 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

Adición de:

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

Del 27 de septiembre al 2023

Cisco Webex

Adición de:

- CSIDL_LOCAL_APPDATA\Programs\Cisco Spark\CiscoCollabHost.exe

Microsoft OneNote

Adición de:

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

Microsoft SQL Server

Adición de:

- 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

Eliminación de:

- 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

Equipos de Microsoft

Adición de:

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

Predeterminado de Microsoft Windows

Adición de:

- CSIDL_WINDOWS\WinSxS*\TiWorker.exe

Desplomarse

Adición de:

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

Symantec Endpoint Protection

Adición de:

- 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

Eliminación de:

- 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\

Nuevas listas creadas

- Conector de cliente Zscaler
- Central de terminales de ManageEngine
- Protección contra pérdida de datos de Symantec

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).