

Cisco-Maintained Exclusion List Changes for Cisco Secure Endpoint Console

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Expectations When You Update](#)

[Changes](#)

[August 28th - 2019](#)

[Microsoft Windows Default:](#)

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

[Docker - Mac:](#)

[New Lists Created:](#)

[September 18th - 2019](#)

[Apple MacOS Default:](#)

[McAfee - Mac](#)

[Cisco Jabber - Mac](#)

[Crashplan - Mac](#)

[JAMF Casper - Mac](#)

[VMWare Fusion - Mac](#)

[Xcode - Mac](#)

[One Drive - Windows](#)

[Citrix ICA Client - Windows](#)

[New Lists Created:](#)

[December 11th - 2019](#)

[One Drive - Windows](#)

[Splunk - Windows](#)

[Splunk - Linux](#)

[New Lists Created:](#)

[February 12th - 2020](#)

[Microsoft Windows Default - Windows](#)

[Websense - Windows](#)

[Microsoft SQL Server - Windows](#)

[June 10th - 2020](#)

[Malwarebytes - Windows](#)

[Microsoft Office - Windows](#)

[IIS - Windows](#)

[Altiris by Symantec - Windows](#)

[McAfee - Windows](#)

[New Lists Created:](#)

[July 15th - 2020](#)

[Domain Controllers - Windows](#)

[Microsoft Teams - Windows](#)

[New List Created](#)

[August 26th - 2020](#)

[Microsoft SQL Server - Windows](#)

[September 30th - 2020](#)

[Malwarebytes - Windows](#)

[Digital Guardian - Mac](#)

[New List Created](#)

[March 3rd - 2021](#)

[Kaspersky - Windows](#)

[SCCM - Windows](#)

[Symantec - Windows](#)

[New Lists Created](#)

[June 30th - 2021](#)

[Microsoft Windows Default](#)

[Citrix ICA Client](#)

[Citrix Provisioning Server](#)

[New Lists Created](#)

[September 29th - 2021](#)

[Cisco Webex - Windows](#)

[Crashplan - Windows](#)

[Crashplan - Mac](#)

[VMware - Windows](#)

[March 23rd - 2022](#)

[Microsoft Windows Default](#)

[Hyper-V - Windows](#)

[Microsoft Windows Defender - Windows](#)

[June 29th - 2022](#)

[Microsoft Windows Default](#)

[Cisco AnyConnect VPN](#)

[Cisco Webex](#)

[Microsoft OneDrive \(Previously One Drive\)](#)

[Tanium - Windows](#)

[Citrix Provisioning Server](#)

[New Lists Created](#)

[Sept 14th - 2022](#)

[Microsoft Windows Default](#)

[Microsoft SQL Server](#)

[TrendMicro / Apex One](#)

[New Lists Created](#)

[October - 2022](#)

[December 14th - 2022](#)

[Microsoft Windows Default](#)

[Backend Changes - Windows](#)

[New Lists Created](#)

[April 12th - 2023](#)

[Microsoft Windows Default](#)

[Microsoft Intune](#)

[McAfee Trellix SolidCore](#)

[Cisco Webex](#)

[Microsoft Defender for MacOS](#)

[Microsoft Defender for Linux](#)

[May 31st - 2023](#)

[VEEAM](#)

[VMWare](#)

[September 27th - 2023](#)

[Cisco Webex](#)

[Microsoft OneNote](#)

[Microsoft SQL Server](#)

[Microsoft Teams](#)

[Microsoft Windows Default](#)

[Splunk](#)

[Symantec Endpoint Protection](#)

[New Lists Created](#)

[November 22nd - 2023](#)

[Microsoft Windows Default](#)

[Citrix ICA Client](#)

[New Lists Created](#)

[January 24th - 2024](#)

[New List Created](#)

[June 19th - 2024](#)

[September 25th - 2024](#)

[Microsoft Teams](#)

Introduction

This document describes the changes added to the Cisco-Maintained Exclusions.

Cisco-Maintained Exclusions are created and maintained by Cisco to provide better compatibility between the Advanced Malware Protection (AMP) for Endpoints Connector and antivirus, security or other software, these exclusions can be added to new versions of an application.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Exclusions in AMP for Endpoints
- AMP console

Components Used

The information in this document is based on these software and hardware versions:

- AMP for Endpoints console version 5.4.20190820

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Expectations When You Update

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.

When the Cisco-Maintained lists are changed, a policy update occurs on the backend to reflect that change. As each of the Endpoints use that list check in on their heartbeat, they pull the updated policy. These policy changes are not reflected in the audit log as it is technically a change to the exclusion list, not the policy itself, and Cisco-maintained exclusion lists do not exist within the normal audit log on individual consoles. For large scale environments, this looks like a flood of policy updates and the end result will be better performance on each of the Endpoints.

The update period depends on each endpoint. If all the machines are online, the updates would take place within 1-2 heartbeats. If this is a global environment, updates continue to occur as machines come online so don't be surprised to see additional policy updates 24-48 hours after the maintained list is pushed.

Changes

August 28th - 2019

Microsoft Windows Default:

Removal of:

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

Reason: Repetitive. Another exclusion in the base set covers it.

Addition of:

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

Reason: Windows 10 updates sporadically failed due to process scans.

N-Able Solar Winds - Windows:

Addition of:

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

Docker - Mac:

Removal of:

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

Reason: Additional test has left us with concerns on security so development has pinpointed better exclusions.

Addition of:

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

New Lists Created:

Linux:

- Docker - Connector 1.10.2
- Docker - Connector 1.11+
- Zabbix

Mac:

- Virtual Box
- Digital Guardian

September 18th - 2019

Apple MacOS Default:

Addition of:

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

McAfee - Mac

Addition of:

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

Cisco Jabber - Mac

Removal of:

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

Reason: Better security and the additional functionality of process-based exclusions.

Addition of:

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

Crashplan - Mac

Addition of:

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

JAMF Casper - Mac

Removal of:

- **/usr/bin/sw_vers**

Reason: Better security and the additional functionality of process-based exclusions.

Addition of:

- **/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

Addition of:

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

Xcode - Mac

Addition of:

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

One Drive - Windows

Minor change:

- **C:*\Users\OneDrive** (Added the backslash for better security)

Citrix ICA Client - Windows

Addition of:

- **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**

Reason: Recent update of Citrix suggested exclusions.

New Lists Created:

Windows

- Citrix Provisioning Server
- Citrix Cloud Connector

December 11th - 2019

One Drive - Windows

Addition of:

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

Splunk - Windows

Addition of:

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

Splunk - Linux

Addition of:

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

New Lists Created:

Azure - Linux

Vagrant - Mac

February 12th - 2020

Microsoft Windows Default - Windows

Addition of:

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

Websense - Windows

Addition of:

- **[Multiple Drives]:\Program Files*\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

Addition of:

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

June 10th - 2020

Malwarebytes - Windows

Minor Change:

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

Microsoft Office - Windows

Addition of:

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

IIS - Windows

Addition of:

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

Altiris by Symantec - Windows

Addition of:

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

McAfee - Windows

Addition of:

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

New Lists Created:

NetScout - Windows

IBM - Windows

July 15th - 2020

Domain Controllers - Windows

Addition of:

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

Microsoft Teams - Windows

Addition of:

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

New List Created

Control Up

August 26th - 2020

**Due to additional testing, the original release date was extended from the 19th to the 26th

Microsoft SQL Server - Windows

Replacing:

- 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

Addition of:

- 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

September 30th - 2020

Malwarebytes - Windows

Addition of:

- CSIDL_PROGRAM_FILES\Malwarebytes' Anti-Malware\mbam.exe
- CSIDL_PROGRAM_FILESEX86\Malwarebytes' Anti-Malware\mbam.exe

Digital Guardian - Mac

Addition of:

- /usr/local/dgagent
- /dgagent

New List Created

Digital Guardian - Windows

March 3rd - 2021

Kaspersky - Windows

Addition of:

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

SCCM - Windows

Removal of:

- WINDOWS\CCM\ServiceData - Duplicate Path
- Program Files\Microsoft Configuration Manager\EasySetupPayload - Duplicate Path

Symantec - Windows

Addition of:

- 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

New Lists Created

Cisco AnyConnect - Windows

Microsoft Defender ATP - Windows

June 30th - 2021

Microsoft Windows Default

Addition of:

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

Citrix ICA Client

Addition of:

- 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

Removal of:

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

Addition of:

- 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

New Lists Created

Commvault - Windows

Citrix Sessions Recording - Windows

September 29th - 2021

Cisco Webex - Windows

Addition of:

- 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

Addition of:

- **CSIDL_PROGRAM_FILES\Code42\Code42Service.exe**

Crashplan - Mac

Addition of:

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

VMware - Windows

Addition of:

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

March 23rd - 2022

Microsoft Windows Default

Addition of:

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

Hyper-V - Windows

Addition of:

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

Microsoft Windows Defender - Windows

Addition of:

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

June 29th - 2022

Microsoft Windows Default

Addition of:

- ***.applocker**

Cisco AnyConnect VPN

Addition of:

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

Cisco Webex

Addition of:

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

Microsoft OneDrive (Previously One Drive)

Addition of:

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

Tanium - Windows

Addition of:

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

Citrix Provisioning Server

Addition of:

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

Removal of:

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

New Lists Created

X1 Search - Windows

Microsoft Intune - Windows

Sept 14th - 2022

Microsoft Windows Default

Addition of:

- **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.exencrypt-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_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

Expanded to include V. 2019

Addition of:

- 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 / Apex One

Addition Of:

- 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

New Lists Created

Azure DevOps - Windows

October - 2022

Through the month of October, malformed exclusions that were introduced to the Secure Endpoint environment during earlier

iterations of the product will be removed from custom exclusion lists. More information related to this initiative can be found [Here](#).

December 14th - 2022

Microsoft Windows Default

Addition of:

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

Backend Changes - Windows

- **csc_ui.exe** added to Exploit Prevention Global Exclusions for V5 and Script Control.

Removal of: [Performance Impacting Exclusions](#)

New Lists Created

1Password - Windows, Mac, Linux

McAfee Trellix SolidCore - Windows

April 12th - 2023

Microsoft Windows Default

Addition of:

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

Removal of:

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

Microsoft Intune

Addition of:

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

McAfee Trellix SolidCore

Minor change:

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

Cisco Webex

Addition of:

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

Microsoft Defender for MacOS

Addition of:

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

Microsoft Defender for Linux

Addition of:

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

May 31st - 2023

VEEAM

Addition of:

- **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

Addition of:

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

September 27th - 2023

Cisco Webex

Addition of:

- **CSIDL_LOCAL_APPDATA\Programs\Cisco Spark\CiscoCollabHost.exe**

Microsoft OneNote

Addition of:

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

Microsoft SQL Server

Addition of:

- **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**

Removal of:

- **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 Teams

Addition of:

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

Microsoft Windows Default

Addition of:

- **CSIDL_WINDOWS\WinSxS*\TiWorker.exe**

Splunk

Addition of:

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

Symantec Endpoint Protection

Addition of:

- **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**

Removal of:

- **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**

New Lists Created

- Zscaler Client Connector
- ManageEngine Endpoint Central
- Symantec Data Loss Protection

November 22nd - 2023

Microsoft Windows Default

Addition of:

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

Citrix ICA Client

Addition of:

- **CSIDL_PROGRAM_FILESX86\Citrix\ICA Client\SelfServicePlugin\SelfService.exe**
- **CSIDL_PROGRAM_FILESX86\Citrix\ICA Client\SelfServicePlugin\SelfServicePlugin.exe**
- **CSIDL_PROGRAM_FILESX86\Citrix\ICA Client\Receiver\FeatureFlag\CWAFeatureFlagUpdater.exe**
- **CSIDL_PROGRAM_FILESX86\Citrix\ICA Client\wfcrun32.exe**
- **CSIDL_PROGRAM_FILESX86\Citrix\ICA Client\Receiver\Receiver.exe**

New Lists Created

- Ivanti LANDesk
- Atera Agent

January 24th - 2024

Microsoft SQL Server and Azure DevOps needed minor adjustments related to changes in exclusion processing for Windows Endpoint 8.2.1+. No exclusions were added.

New List Created

- Arctic Wolf

June 19th - 2024

In order to maximize compatibility with Microsoft Windows Secure Endpoint versions, modifications to existing exclusions starting with **CSIDL_Windows...** will be changed to **[Any Drive]:\Windows....** The following Windows exclusion lists will be impacted with the change:

- Altiris by Symantec
- Avast
- Citrix Provisioning Server
- Diebold Warsaw
- Domain Controller
- IIS
- Malwarebytes
- Microsoft Intune
- Microsoft SQL Server
- Microsoft Windows Default
- VEEAM

September 25th - 2024

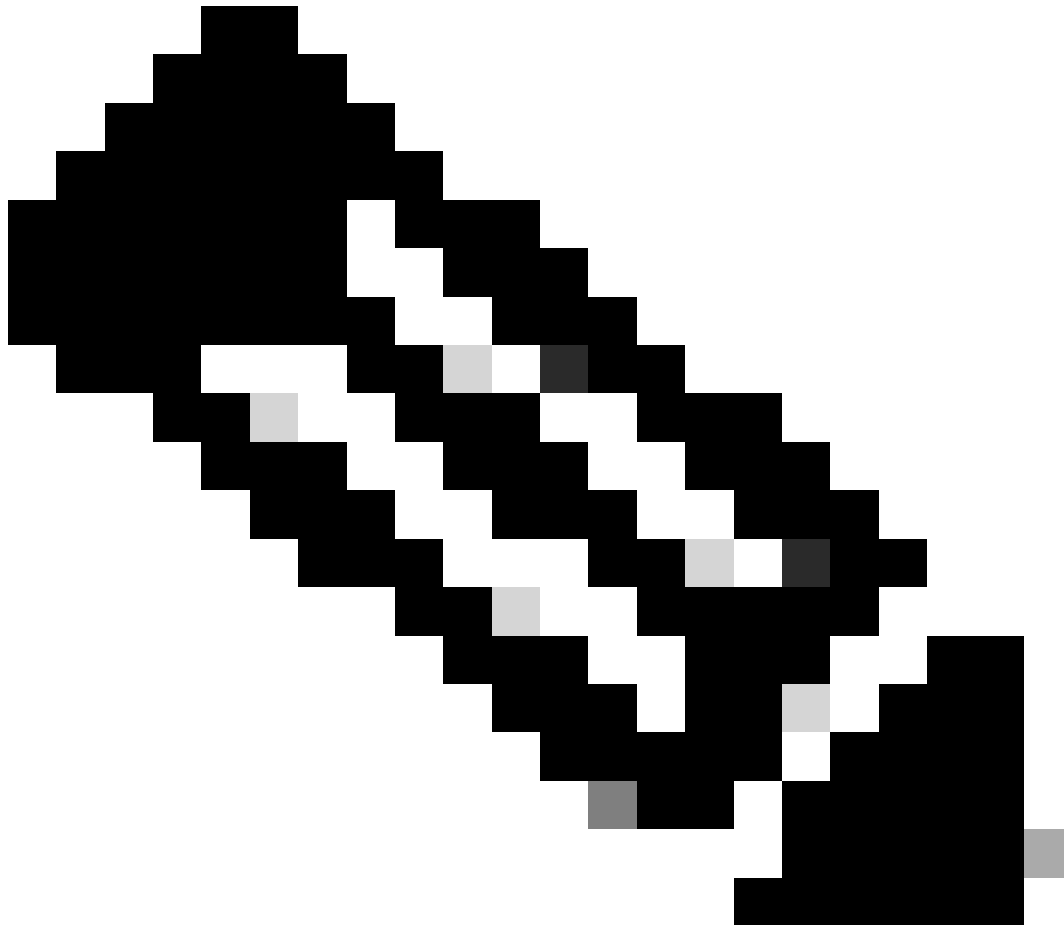
Microsoft Teams

addition of:

CSIDL_PROGRAM_FILES\WindowsApps\ MSTeams_*\ms-teams.exe

CSIDL_PROGRAM_FILES\WindowsApps\ MSTeams_*\ms-teamsupdate.exe

CSIDL_PROGRAM_FILES\WindowsApps\ MSTeams_*\msedgewebview2.exe



Note: Windows Secure Endpoint Versions 8.4.0+ resolves pathing for all CSIDL exclusions.
