# 思科维护的思科安全终端控制台的排除列表更改

## 目录


简介

先决条件

- 要求
- 使用的组件

更新时的期望

更改

- 2019年8月28日
  - Microsoft Windows默认值：
  - N-Able Solar Winds — 窗户：
  - Docker - Mac:
  - 新建列表：
- 9月18日 — 2019年
  - Apple MacOS默认值：
  - McAfee - Mac
  - Cisco Jabber - Mac
  - 崩溃计划 — Mac
  - JAMF Casper - Mac
  - VMWare Fusion - Mac
  - Xcode - Mac
  - 一个驱动器 — Windows
  - Citrix ICA客户端 — Windows
  - 新建列表：
- 12月11日 — 2019年
  - 一个驱动器 — Windows
  - Splunk - Windows
  - Splunk - Linux
  - 新建列表：
- 2月12日 — 2020年
  - Microsoft Windows默认值 — 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
  - 新建列表：
- 7月15日 — 2020年
  - 域控制器 — Windows
  - Microsoft Teams - Windows
  - 已创建新列表
- 8月26日 — 2020年
  - Microsoft SQL Server - Windows

- 9月30日 — 2020年
  - Malwarebytes - Windows
  - Digital Guardian - Mac
  - 已创建新列表
- 2021年3月3日
  - 卡巴斯基 — Windows
  - SCCM - Windows
  - Symantec - Windows
  - 已创建新列表
- 2021年6月30日
  - Microsoft Windows默认值
  - Citrix ICA客户端
  - Citrix调配服务器
  - 已创建新列表
- 9月29日 — 2021年
  - Cisco Webex - Windows
  - 崩溃计划 — Windows
  - 崩溃计划 — Mac
  - VMware - Windows
- 2022年3月23日
  - Microsoft Windows默认值
  - Hyper-V - Windows
  - Microsoft Windows Defender - Windows
- 2022年6月29日
  - Microsoft Windows默认值
  - Cisco AnyConnect VPN
  - Cisco Webex
  - Microsoft OneDrive（以前是一个驱动器）
  - Tanium - Windows
  - Citrix调配服务器
  - 已创建新列表
- 9月14日 — 2022年
  - Microsoft Windows默认值
  - Microsoft SQL 服务器
  - TrendMicro / Apex One
  - 已创建新列表
- 2022年10月
- 12月14日 — 2022年
  - Microsoft Windows默认值
  - 后端更改 — Windows
  - 已创建新列表
- 4月12日 — 2023年
  - Microsoft Windows默认值
  - Microsoft Intune
  - McAfee Trellix SolidCore
  - Cisco Webex
  - 适用于MacOS的Microsoft Defender
  - Microsoft Defender for Linux
- 5月31日 — 2023年
  - VEEAM
  - VMWare

9月27日 — 2023年
Cisco Webex
Microsoft OneNote
Microsoft SQL 服务器
Microsoft Teams
Microsoft Windows默认值
Splunk
Symantec Endpoint Protection
已创建新列表
11月22日 — 2023年
Microsoft Windows默认值
Citrix ICA客户端
已创建新列表
1月24日 — 2024年
已创建新列表

# 简介

本文档介绍添加到思科维护的例外项中的更改。

思科维护的例外项由思科创建和维护，以在面向终端的高级恶意软件防护(AMP)连接器与防病毒、安全或其他软件之间提供更好的兼容性，这些例外项可添加到应用的新版本中。

# 先决条件

## 要求

Cisco 建议您了解以下主题：

- 面向终端的AMP中的排除项
- AMP控制台

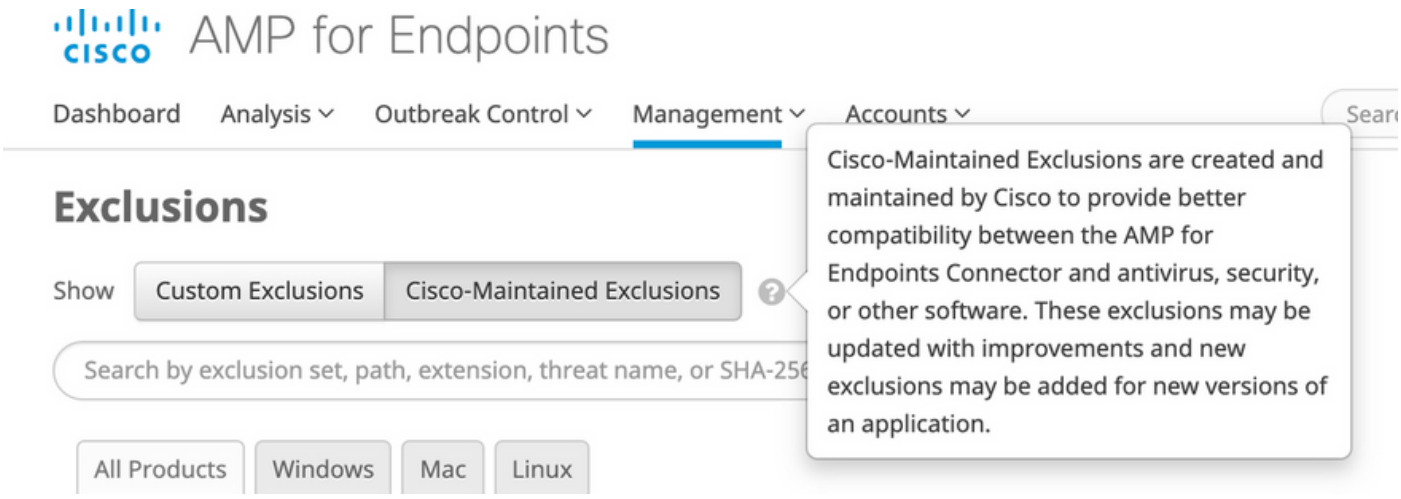
## 使用的组件

本文档中的信息基于以下软件和硬件版本：

- 面向终端的AMP控制台版本5.4.20190820

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

# 更新时的期望




当思科维护的列表发生更改时，将在后端进行策略更新以反映该更改。 当每个终端都使用该列表签入其心跳时，它们会提取更新的策略。 这些策略更改不会反映在审核日志中，因为从技术上讲，这是对排除列表的更改，而不是策略本身，并且思科维护的排除列表在单个控制台的正常审核日志中不存在。 对于大规模环境，这看起来像是大量策略更新，最终结果将是每个端点上的性能更好。

更新周期取决于每个端点。 如果所有机器都联机，则将在1-2个心跳内进行更新。 如果是在全球环境下，当计算机联机时，更新会继续进行，因此，在推送维护列表后的24-48小时内，不要惊讶地看到其他策略更新。

# 更改

## 2019年8月28日

Microsoft Windows默认值：

删除：

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

原因：重复性。基本套中的另一个排除项包括它。

增加：

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

原因：由于进程扫描，Windows 10更新偶尔失败。

N-Able Solar Winds — 窗户：

增加：

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

Docker - Mac:

删除：

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

原因: 额外的测试让我们对安全问题有所担忧，因此开发工作可以找到更好的排除方法。

增加：

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

新建列表：

Linux:

- Docker — 连接器1.10.2
- Docker — 连接器1.11+
- 扎比克斯

MAC :

- 虚拟盒
- 数字保护者

## 9月18日 — 2019年

Apple MacOS默认值：

增加：

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

McAfee - Mac

增加：

- /Library/McAfee/Agent/bin/CmdAgent

**Cisco Jabber - Mac**

删除：

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

原因：安全性更高，基于流程的排除功能更多。

增加：

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

崩溃计划 — Mac

增加：

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

JAMF Casper - Mac

删除：

- /usr/bin/sw_vers

原因：安全性更高，基于流程的排除功能更多。

增加：

- /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

增加：

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

Xcode - Mac

增加：

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

一个驱动器 — Windows

细微更改：

- C:*\Users\OneDrive\ (添加反斜线以提高安全性)

Citrix ICA客户端 — Windows

增加：

- 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建议的例外项。

新建列表：

Windows 窗口版本

- Citrix调配服务器
- Citrix云连接器

## 12月11日 — 2019年

一个驱动器 — Windows

增加：

- CSIDL_LOCAL_APPDATA\Microsoft\OneDrive\OneDrive.exe

Splunk - Windows

增加：

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

Splunk - Linux

增加：

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

新建列表：

Azure - Linux

Vagrant - Mac

## 2月12日 — 2020年

Microsoft Windows默认值 — Windows

增加：

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

Websense - Windows

增加：

- [多个驱动器]:\Program Files*\Websense\
- C:\Program文件(x86)\Websense\Websense Endpoint\dserui.exe
- C:\Program Files\Websense\Websense Endpoint\dserui.exe
- C:\Program文件(x86)\Websense\Websense Endpoint\EndPointClassifier.exe
- C:\Program文件(x86)\Websense\Websense Endpoint\FilterSDK\kvoop.exe
- C:\Program文件(x86)\Websense\Websense Endpoint\wepsvc.exe

Microsoft SQL Server - Windows

增加：

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

## 2020年6月10日

Malwarebytes - Windows

### 细微更改：

- C:\ProgramData\Malwarebytes终端代理\
- C:\ProgramData\Malwarebytes\MBAMService\

### Microsoft Office - Windows

### 增加：

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

IIS - Windows

### 增加：

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

Altiris by Symantec - Windows

### 增加：

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

McAfee - Windows

增加：

- C:\Program Files\McAfee\Endpoint安全\自适应威胁防护\mfeatp.exe

新建列表：

NetScout - Windows

IBM - Windows

## 7月15日 — 2020年

域控制器 — Windows

增加：

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

Microsoft Teams - Windows

增加：

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

已创建新列表

控制打开

## 8月26日 — 2020年

**由于进行额外测试，原发布日期从19日延长至26日

Microsoft SQL Server - Windows

替换：

- 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

增加：

- 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

增加：

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

Digital Guardian - Mac

增加：

- /usr/local/dgagent
- /dgagent

已创建新列表

Digital Guardian - Windows

## 2021年3月3日

卡巴斯基 — Windows

增加：

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

SCCM - Windows

删除：

- WINDOWS\CCM\ServiceData — 重复路径

- 程序文件\Microsoft Configuration Manager\EasySetupPayload -重复路径

Symantec - Windows

增加：

- 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

已创建新列表

Cisco AnyConnect - Windows

Microsoft Defender ATP - Windows

## 2021年6月30日

Microsoft Windows默认值

增加：

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

Citrix ICA客户端

增加：

- 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客户端\

Citrix调配服务器

删除：

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

增加：

- 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

已创建新列表

Commvault - Windows

Citrix会话记录 — Windows

## 9月29日 — 2021年

Cisco Webex - Windows

增加：

- 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_*\

崩溃计划 — Windows

增加：

- CSIDL_PROGRAM_FILES\Code42\Code42Service.exe

崩溃计划 — Mac

增加：

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

VMware - Windows

增加：

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

## 2022年3月23日

Microsoft Windows默认值

### 增加：

- C:\Windows\System32\SearchIndexer.exe

Hyper-V - Windows

增加：

- CSIDL_COMMON_APPDATA\Microsoft\Windows\Hyper-V\
- CSIDL_COMMON_DOCUMENTS\Hyper-V\虚拟硬盘\

Microsoft Windows Defender - Windows

增加：

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

## 2022年6月29日

Microsoft Windows默认值

增加：

- *.applocker

Cisco AnyConnect VPN

增加：

- CSIDL_PROGRAM_FILESX86\Cisco\Cisco AnyConnect安全移动客户端\acwebhelper.exe

Cisco Webex

增加：

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

Microsoft OneDrive（以前是一个驱动器）

增加：

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

Tanium - Windows

增加：

- C:\Program文件(x86)\Tanium\Tanium最终用户通知工具\bin\end-user-notifications.exe

Citrix调配服务器

增加：

- CSIDL_PROGRAM_FILES\Citrix\Provisioning Services\MgmtDaemon.com

删除：

- CSIDL_PROGRAM_FILES\Citrix\Provisioning Services\MgmntDaemon.com

已创建新列表

X1搜索 — Windows

Microsoft Intune - Windows

## 9月14日 — 2022年

Microsoft Windows默认值

增加：

- 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 服务器

扩展至包括V. 2019

增加：

- 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

添加：

- 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

已创建新列表

Azure DevOps - Windows

## 2022年10月

在10月内，在产品早期迭代期间引入到安全终端环境的格式错误的排除将从自定义排除列表中删除。 有关本计划的更多信息，请访问此处。

## 12月14日 — 2022年

Microsoft Windows默认值

增加：

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

后端更改 — Windows

- csc_ui.exe 添加到V5和脚本控制的漏洞防御全局排除。

删除：影响性[能的例外项]

已创建新列表

1密码 — Windows、Mac、Linux

McAfee Trellix SolidCore - Windows

## 4月12日 — 2023年

Microsoft Windows默认值

增加：

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

删除：

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

Microsoft Intune

增加：

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

McAfee Trellix SolidCore

细微更改：

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

Cisco Webex

增加：

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

适用于MacOS的Microsoft Defender

增加：

- /Library/Application Support/Microsoft/Defender/

Microsoft Defender for Linux

增加：

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

## 5月31日 — 2023年

VEEAM

增加：

- 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

增加：

- 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

增加：

- CSIDL_LOCAL_APPDATA\Programs\Cisco Spark\CiscoCollabHost.exe

Microsoft OneNote

增加：

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

Microsoft SQL 服务器

增加：

- 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 Teams

增加：

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

Microsoft Windows默认值

增加：

- CSIDL_WINDOWS\WinSxS*\TiWorker.exe

Splunk

增加：

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

Symantec Endpoint Protection

增加：

- 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

删除：

- 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\

已创建新列表

- Zscaler客户端连接器
- 管理引擎终端中心
- Symantec数据丢失保护

11月22日 — 2023年

Microsoft Windows默认值

增加：

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

Citrix ICA客户端

增加：

- 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

已创建新列表

- Ivanti LANDesk
- Atera代理

1月24日 — 2024年

Microsoft SQL Server和Azure DevOps需要与Windows终结点8.2.1+的排除处理更改相关的细微调整。未添加任何排除项。

已创建新列表

- 北极狼

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。