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

- 12月18日 — 2024年
  - VEEAM
  - Cisco Webex
- 2025年6月4日
  - Microsoft Windows默认值
  - Apple macOS默认值
- 9月17日 — 2025年
  - Microsoft Windows默认值
  - Apple macOS默认值
- 12月17日 — 2025年
  - Microsoft Teams
- 2026年2月4日
  - Microsoft Windows默认值
  - Microsoft Exchange 服务器
  - Appsense
- 2026年9月23日
  - Windows默认值
  - Splunk - Windows
  - Hyper-V - Windows

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

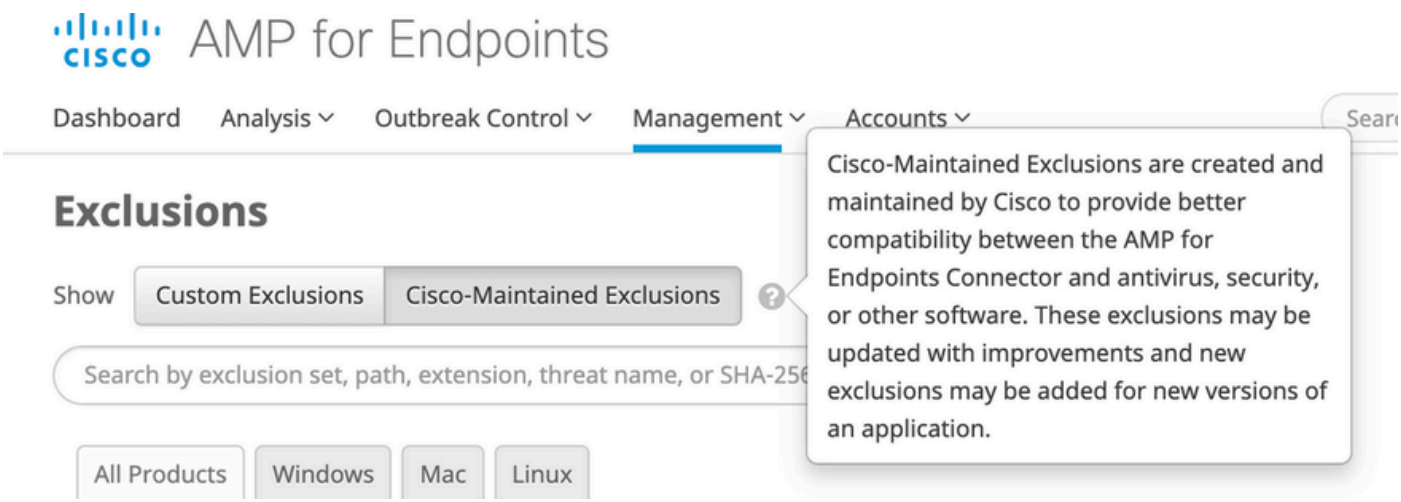
使用的组件

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

12月18日 — 2024年

VEEAM

增加：

- CSIDL_PROGRAM_FILES\Veeam\Backup and Replication\Threat Hunter\

Cisco Webex

增加：

- CSIDL_LOCAL_APPDATA\WebEx\WebEx64\Meetings\webexmta.exe
- CSIDL_PROGRAM_FILES\Cisco Spark\CiscoCollabHost.exe

Microsoft Windows默认值

对现有进程omadmclient.exe进行小幅调整，以包含子进程。

2025年6月4日

Microsoft Windows默认值

添加：

- 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\EVM\bin\csc_evm.exe
- CSIDL_PROGRAM_FILES\Microsoft Device Inventory Agent\InventoryService\InventoryService.exe
- CSIDL_PROGRAM_FILESX86\Cisco\Cisco Secure Client\NVM\acnvmagent.exe
- CSIDL_COMMON_APPDATA\Cisco\Cisco Secure Client\EVM*
- CSIDL_PROGRAM_FILES\Microsoft Device Inventory Agent\InventoryService\

Apple macOS默认值

添加：

- /opt/cisco/secureclient/evm/bin/csc_evm.app/Contents/MacOS/csc_evm
- /Library/Cisco/evm/Log Files
- /Library/Cisco/evm/Upload\ Queue/

9月17日 — 2025年

Microsoft Windows默认值

添加：

- CSIDL_PROGRAM_FILES\Cisco\Forensics\AIR\网站**
- CSIDL_PROGRAM_FILES\Cisco\Forensics\AIR\

Apple macOS默认值

添加：

- /opt/cisco/forensics/air/
- /opt/cisco/forensics/air/**

注意：Windows安全终端版本8.4.0+为所有CSIDL例外项解析路径。

12月17日 — 2025年

Microsoft Teams

添加：

- CSIDL_PROGRAM_FILES\WindowsApps\MSTeams_*\

2026年2月4日

Microsoft Windows默认值

添加：

- CSIDL_PROGRAM_FILESX86\Cisco\Cisco Secure Client**

Microsoft Exchange 服务器

添加：

- CSIDL_PROGRAM_FILES\Microsoft\Exchange Server**

Appsense

添加：

- CSIDL_PROGRAM_FILES\AppSense\Environment Manager\Agent\EmSystem.exe

2026年9月23日

Windows默认值

添加：

- CSIDL_PROGRAM_FILES\Orbital\

Splunk - Windows

添加：

- CSIDL_PROGRAM_FILES\SplunkUniversalForwarder\bin\splunk-winevtlog.exe
- CSIDL_PROGRAM_FILES\SplunkUniversalForwarder\bin\splunkd.exe

Hyper-V - Windows

添加：

- C:\ClusterStorage\
- CSIDL_WINDOWS\集群\
- CSIDL_WINDOWS\Cluster\clussvc.exe
- CSIDL_WINDOWS\Cluster\rhs.exe

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）。