安全终端软件支持策略

目录

简介

支持策略

- 标准支持策略
- 长期支持(LTS)政策
  - 连接器
  - 私有云
- 例外
  - 预发行安全终端软件版本
  - 一次性删除

使用超出支持策略的安全终端软件

附录 A：识别部署的不受支持的安全终端连接器

附录 B：安全终端软件支持策略修订历史记录表

简介

本文档介绍思科安全终端软件的支持策略。

此支持政策自2026年7月7日起生效。

支持策略

思科的安全终端软件支持策略适用于：

- 适用于Windows、Linux和macOS的安全终端连接器软件。
- 安全终端私有云软件。

思科的安全终端软件支持策略不适用于：

- 私有云设备硬件。有关私有云设备硬件支持，请参阅思科的生命周期终止策略。
- iOS和Android安全终端连接器。Apple App Store和Google Play商店分别仅提供适用于iOS和Android的最新可用安全终端连接器版本。

标准支持策略

思科将通过技术支持中心(TAC)和安全终端软件的漏洞修复提供技术支持，每个软件版本发布后至少持续一年。在此期限之后，将不再支持该版本用于未来的漏洞修复，但专门为旧版操作系统支持发布的软件版本除外。如果您遇到不支持软件版本的问题，可能会要求您验证较新的维护版本还是最新版本解决了您的问题。

所有操作系统上的安全终端软件支持都将与供应商发布的终止支持计划保持一致。当供应商发布的

扩展支持开始时，安全终端标准支持策略将结束，并由长期支持(LTS)策略取代。LTS不适用于供应商不提供扩展支持的操作系统，例如macOS。

安全终端软件版本可能需要操作系统补丁或升级到更新版本，以满足兼容性、访问所有功能或漏洞修复的需要。

安全终端控制台显示受官方支持的安全终端软件版本。当不再支持软件时，可以从控制台删除软件版本。

安全终端和安全终端私有云连接器按不同的计划发布。请参阅每种部署类型的版本说明，以确定最近受支持的安全终端连接器版本：

- 安全终端私有云版本说明
- 安全终端版本说明

长期支持(LTS)政策

安全终端LTS策略在供应商发布的延长支持期开始时开始。思科要求客户维护所有必要的扩展支持合同，以确保终端操作系统具有有效的供应商支持。在LTS期间，思科通过TAC、漏洞修复和安全终端软件补丁提供技术支持。

对安全终端软件版本的支持仅限于关键维护版本和安全补丁，它们不包含新功能。

客户需要为其旧操作系统安装最新更新补丁并将安全终端LTS软件更新至最新版本，才能获得技术支持。

连接器

有关特定操作系统支持和不支持的安全终端连接器软件的详细信息，请参阅以下文档。

Windows 窗口版本

- 思科安全终端Windows连接器操作系统兼容性

Linux

- Cisco Secure Endpoint Linux Connector OS兼容性
- 思科安全终端Linux连接器长期支持

MAC

- 思科安全终端Mac连接器操作系统兼容性

私有云

有关受支持和不受支持的私有云软件的详细信息，请参阅以下文档：

- 面向终端的AMP/安全终端私有云版本的支持终止公告

例外

预发行安全终端软件版本

预发行版本（如betas和早期现场测试）不遵循标准支持政策。预发行软件的部署在参与期间受相应协议的支持和监管。除非计划协议明确定义，否则不为软件的预发行版本提供技术支持。

对预发行版本提供的任何支持将在相关正式发行版本推出后终止。希望在试用版结束之后使用新功能的客户需要迁移到公开可用且官方支持的安全终端软件版本。

一次性删除

虽然思科会尽一切努力避免这种情况，但由于现场出现问题的严重性或频率，可能需要删除已发布的安全终端软件版本，或解决安全问题。在这种情况下，思科可能会删除安全终端软件版本并执行以下操作之一：

1. 提供可解决这些问题的新版本。
2. 提供客户应升级至哪个版本的建议。

如果安全终端软件版本被删除，将无法下载。对于连接器软件，删除的版本不可配置用于通过策略设置进行升级。这些更改可能需要计划发布私有或公共安全终端控制台或私有云软件，并会尽早提供。

使用超出支持策略的安全终端软件

思科建议客户将安全终端软件升级到最新版本，以确保访问最新功能和安全补丁。在支持策略不再支持安全终端云或安全终端私有云后，思科无法保证安全终端软件将继续运行并连接到这些云，因为它们可能不再兼容最新的云技术。

不受支持的安全终端连接器版本将从安全终端控制台中删除，并且不再可用于通过连接器策略设置进行部署。配置为升级到不受支持的连接器版本的安全终端连接器策略将自动更新以删除配置。

由于缺少较新版本中可用的功能，仍在使用的不受支持的安全终端软件可能会在较低容量下运行，还可能包含未解决的安全问题。在支持结束之前下载的任何安全终端软件安装程序包都不应在支持结束之后安装。

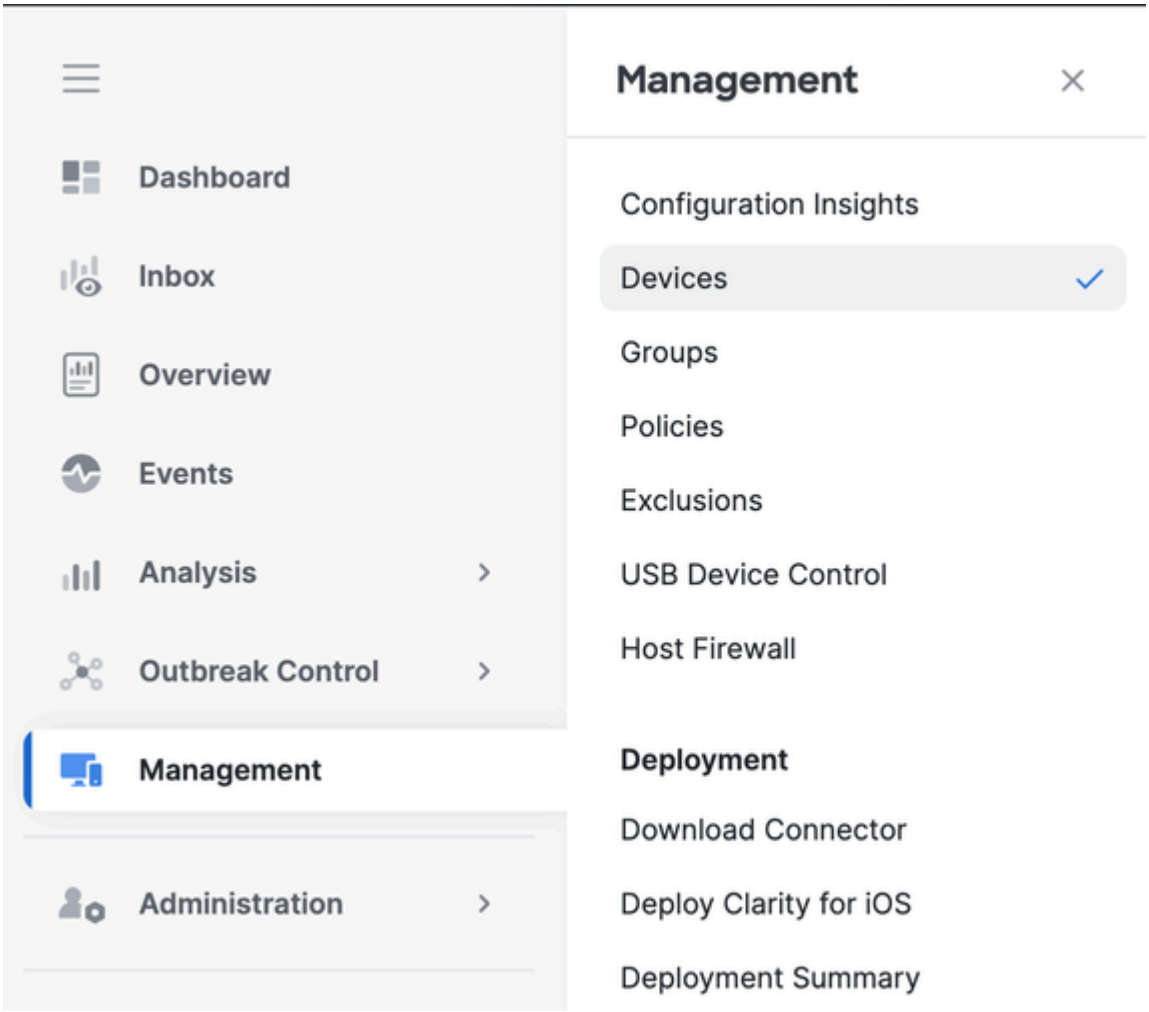
有关当前支持的分发的详细信息，请参阅每个安全终端连接器软件OS兼容性文章：

- 思科安全终端Windows连接器操作系统兼容性
- Cisco Secure Endpoint Linux Connector OS兼容性
- 思科安全终端Mac连接器操作系统兼容性

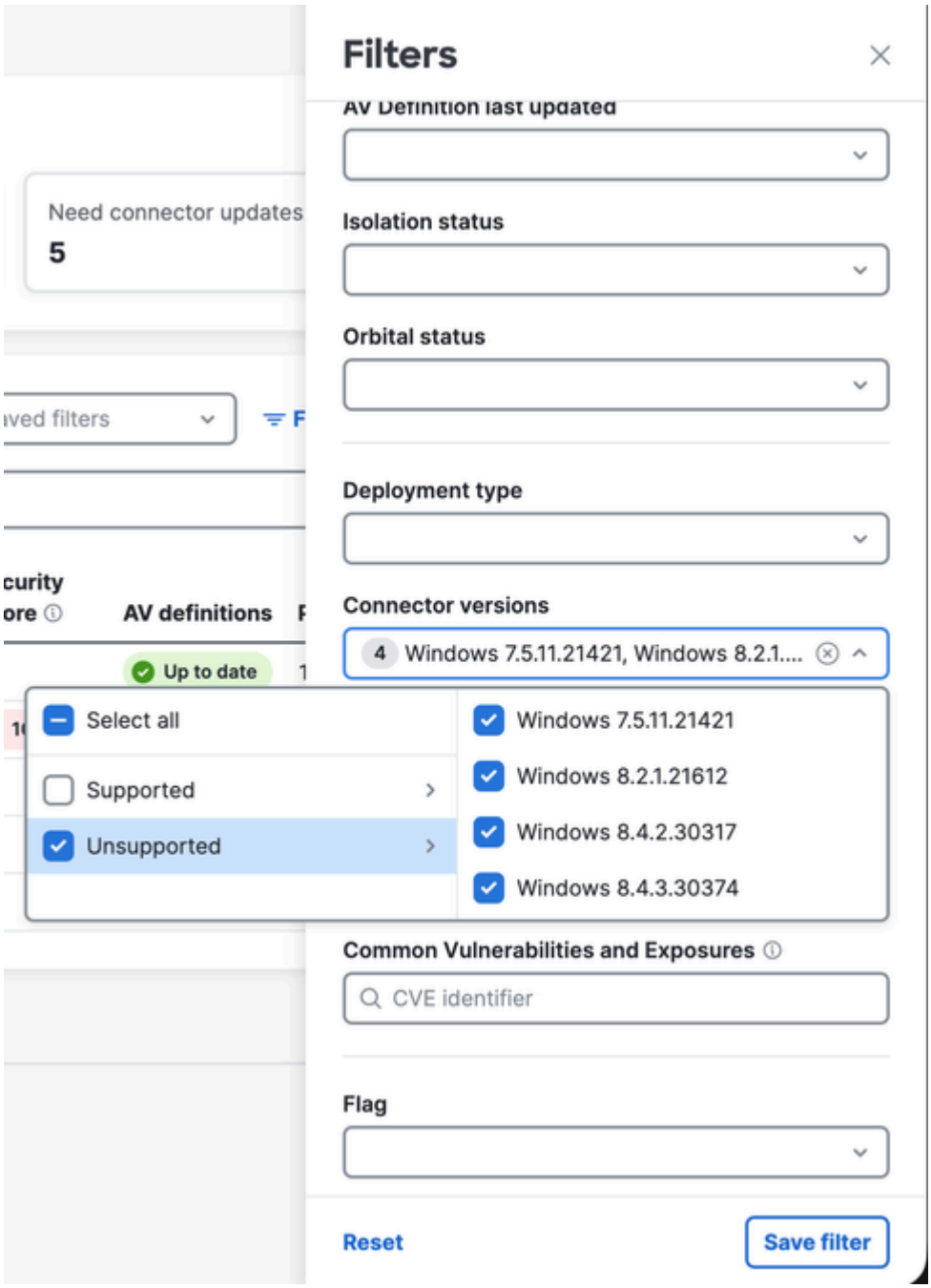
附录 A：识别部署的不受支持的安全终端连接器

在安全终端控制台中可以识别当前部署的不受支持的安全终端连接器：

1. 选择`Management` -> `Devices`，导航到Device Management页面。



2. 展开过滤器，然后从“连接器版本”下拉菜单中选择不受支持。单击Save Filter。



这将显示当前运行不受支持的连接器版本的所有设备。

附录 B：安全终端软件支持策略修订历史记录表

修订版	发布日期	备注
4.0	2026年6月30日	更新了发行说明和操作系统兼容性图表的链接。已更新屏幕截图，以反映控制台中的更改。

3.0	2024年 2月21日	将策略重组为以下部分：标准支持策略和LTS支持策略。删除了FAQ部分。使支持策略更通用以应用于私有云和连接器。
2.0	2022年 8月01日	更新了确定连接器软件支持终止的流程，从基于版本的支持策略转变为基于时间的支持策略。此策略现在适用于私有云软件、私有云虚拟设备和所有连接器操作系统。添加了对旧版操作系统的支持语言。更新的常见问题。
1.0	2020年 4月7日	初始发布

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）。