

# 安全终端-连接器更新因Microsoft攻击面减少而被阻止

## 目录

[简介](#)

[问题](#)

[解决方法](#)

## 简介

本文档介绍在由Microsoft Intune管理的系统上使用复制或模拟系统工具功能的Microsoft Intune攻击表面缩减阻止导致安全终端更新失败所导致的问题。

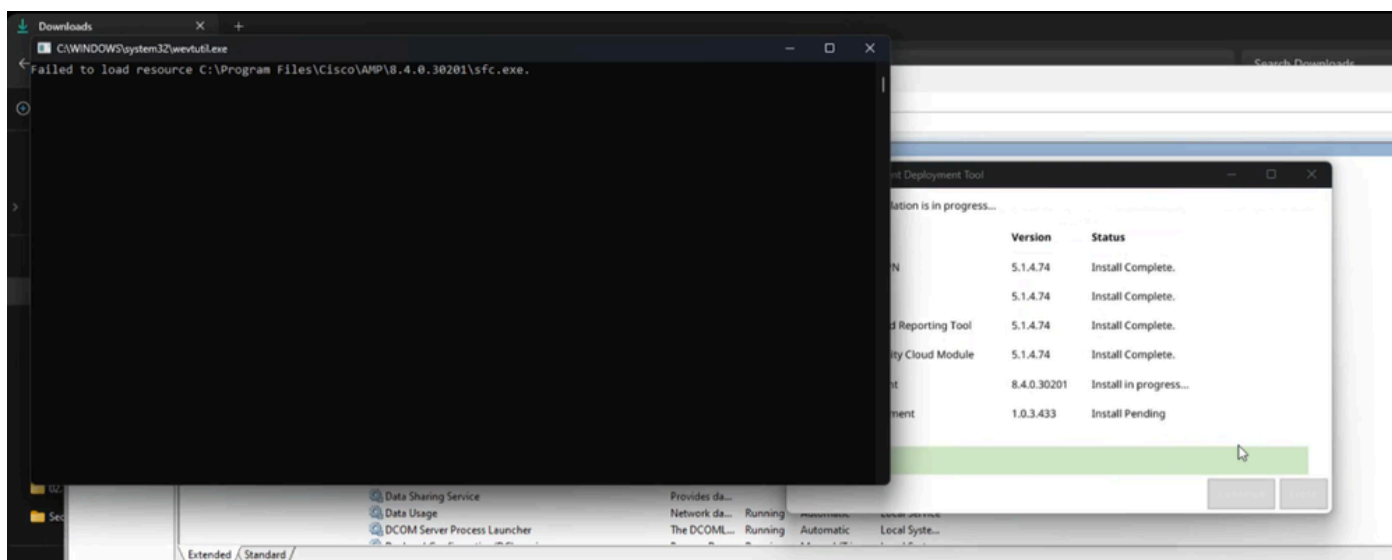
请参阅功能文档：<https://learn.microsoft.com/en-us/defender-endpoint/attack-surface-reduction>

## 问题

我们可能会遇到安全终端升级或安装问题，这些问题由以下错误和指示符表示。

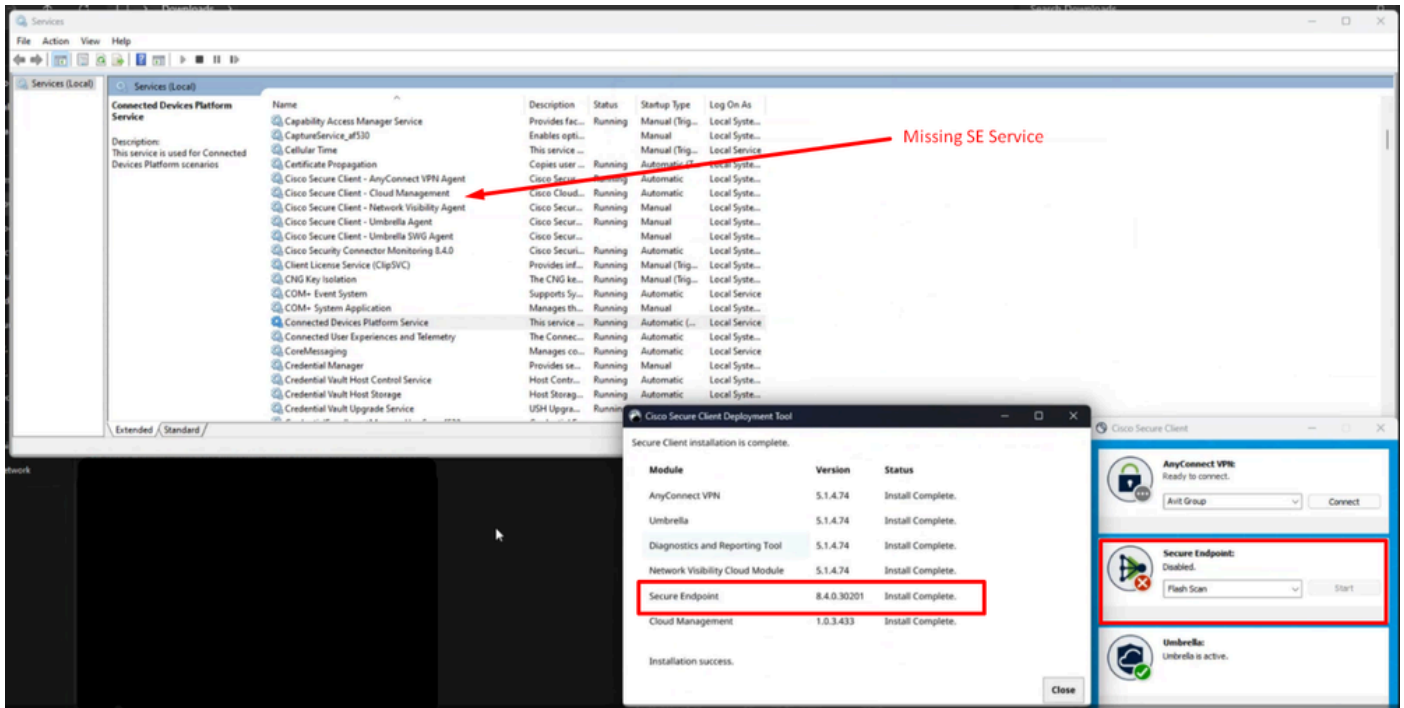
有多种指示器可用于识别此功能是否干扰安全终端更新。

指示器#1：在部署过程中，我们会在安装结束时看到此弹出窗口。请注意，此弹出窗口速度相当快，安装完成后，不会出现其他任何错误记录。

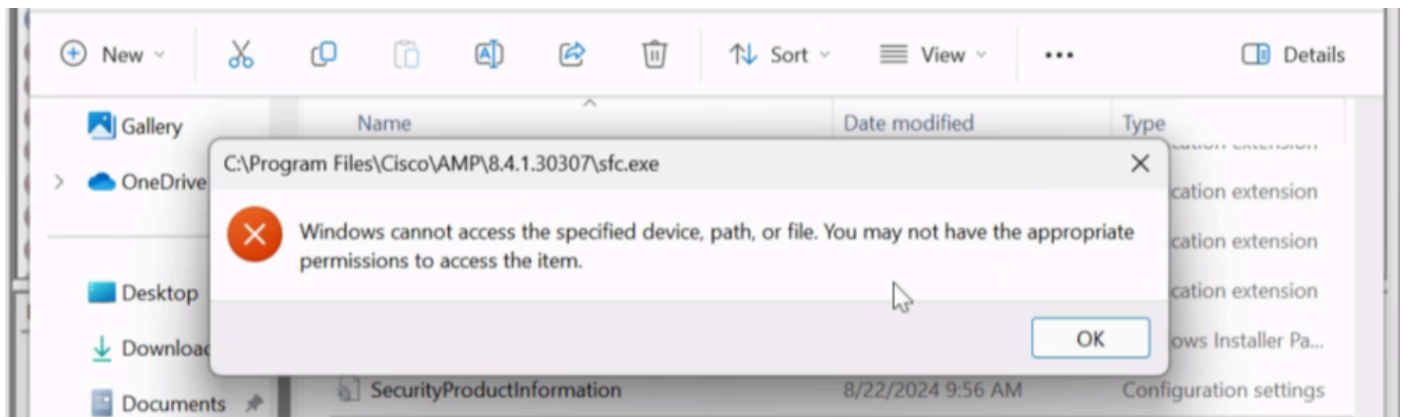


指示器#2：安装后，请注意UI中的安全终端处于禁用状态。

此外，任务管理器—> Services中完全缺少Secure Endpoint Service (sfc.exe)。



指示器#3：如果我们导航到C:\Program Files\Cisco\AMP\version下的思科安全终端位置并尝试手动启动服务，您将获得权限访问被拒绝，即使对本地管理员帐户也是如此



指示符#4：如果我们检查诊断包中的impro\_install.log，我们可以看到类似于以下输出的类似拒绝访问行为。

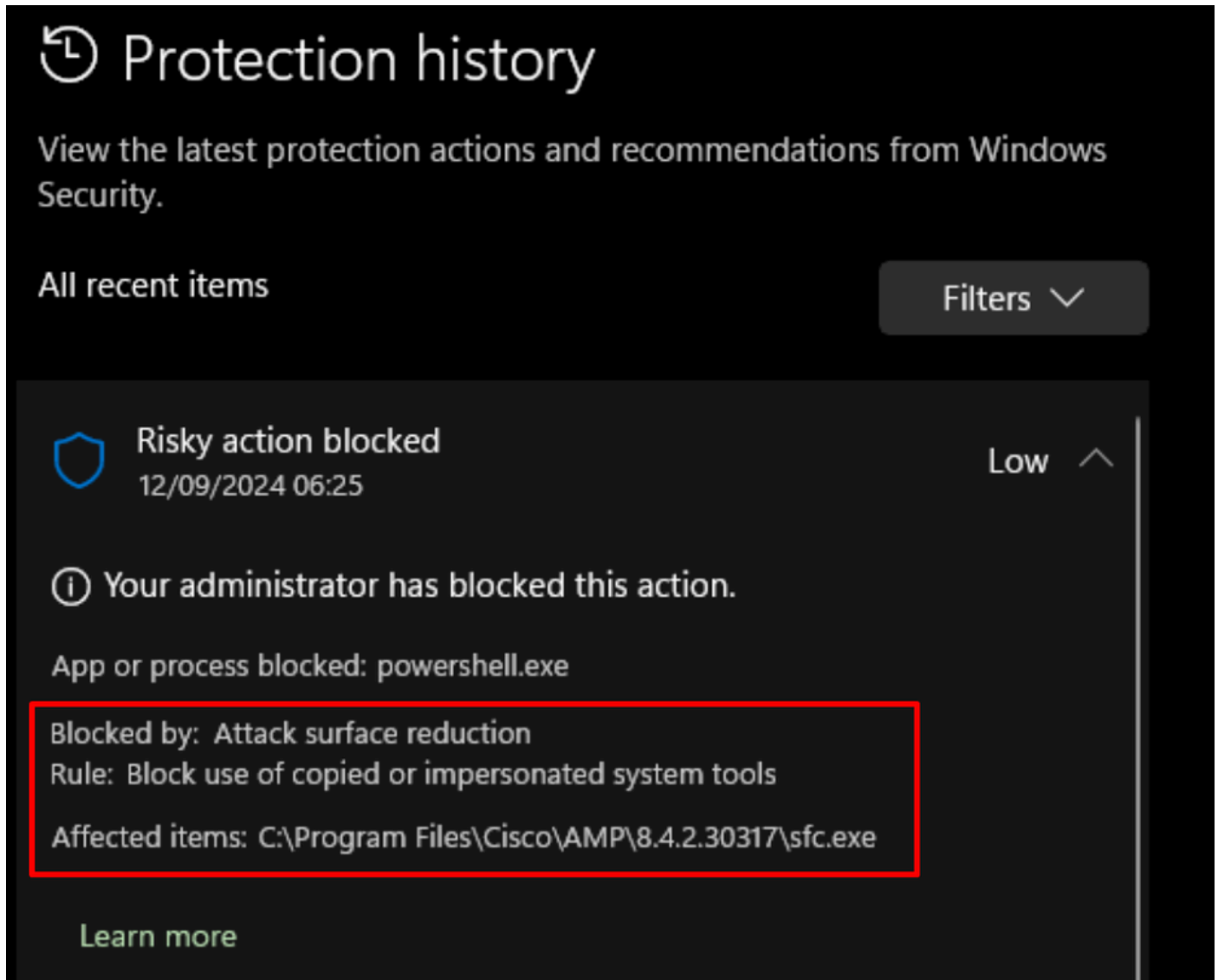
Example #1:

```
(5090625, +0 ms) Aug 22 09:56:33 [17732]: ERROR: Util::GetFileSHA256: unable to generate file fp: C:\Pr  
(5090625, +0 ms) Aug 22 09:56:33 [17732]: ERROR: VerifyFile: Failed to grab hash of C:\Program Files\Ci  
(5090625, +0 ms) Aug 22 09:56:33 [17732]: ERROR: VerifyAllInstalledFiles: Failed to verify $AMP_INSTALL
```

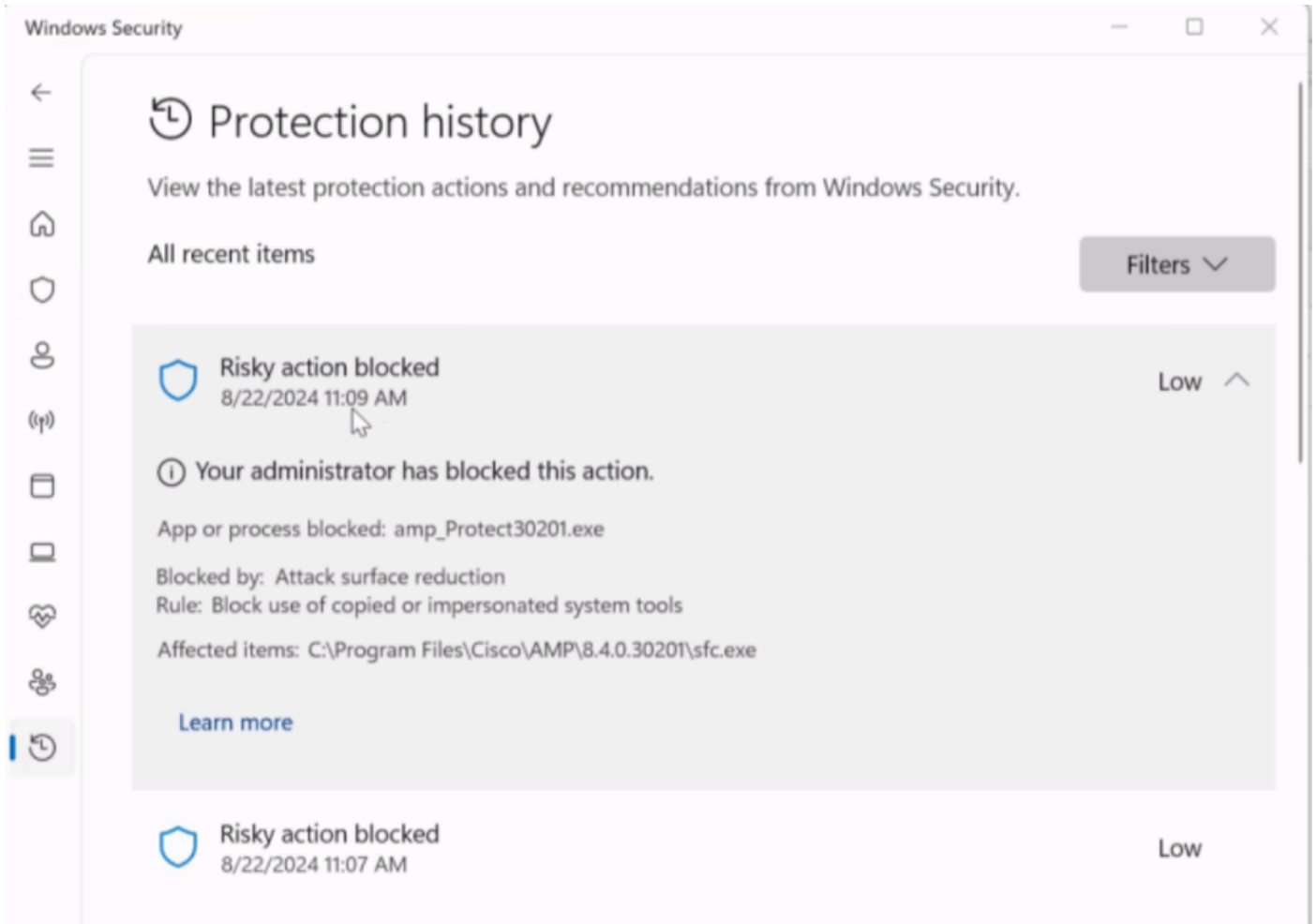
Example #2:

```
(1737859, +0 ms) Sept 11 14:04:05 [20180]: ERROR: imn_error: fp_gen_internal: failed to open file C:\Pr  
(1737859, +0 ms) Sept 11 14:04:05 [20180]: ERROR: Util::GetFileSHA256: unable to generate file fp: C:\P  
(1737859, +0 ms) Sept 11 14:04:05 [20180]: ERROR: VerifyFile: Failed to grab hash of C:\Program Files\C  
(1737859, +0 ms) Sept 11 14:04:05 [20180]: ERROR: VerifyAllInstalledFiles: Failed to verify $AMP_INSTAL
```

指示符#5：如果导航到Windows安全下并查看保护历史记录日志，请查找这些类型的日志消息。



The screenshot displays the 'Protection history' window in Windows Security. The title bar reads 'Protection history' with a refresh icon. Below the title, it says 'View the latest protection actions and recommendations from Windows Security.' There are two tabs: 'All recent items' and 'Filters' (with a dropdown arrow). The main content area shows a single event: 'Risky action blocked' with a shield icon, dated '12/09/2024 06:25', and a severity of 'Low' with an upward arrow. Below the event title is an information icon and the text 'Your administrator has blocked this action.' Underneath, it states 'App or process blocked: powershell.exe'. A red rectangular box highlights the following details: 'Blocked by: Attack surface reduction', 'Rule: Block use of copied or impersonated system tools', and 'Affected items: C:\Program Files\Cisco\AMP\8.4.2.30317\sfc.exe'. At the bottom left, there is a 'Learn more' link.



所有这些都表示安全终端正被第三方应用阻止。在此场景中，在Intune托管终端上发现问题，其中配置了错误或未配置攻击面减少-阻止使用复制或模拟的系统功能。

## 解决方法

建议与应用程序开发人员协商此功能的配置，或者通过此[知识库](#)进一步协商此功能。

为立即进行补救，我们可以将受管终端移至intune中限制较少的策略，或者暂时显式关闭此功能，直到执行正确的步骤。

这是Intune管理员门户下的设置，用作恢复安全终端连接的临时措施。

## Edit profile - WCS - Defender Baseline

Settings catalog

Block Office communication application from creating child processes

Block all Office applications from creating child processes

Block Adobe Reader from creating child processes

Block credential stealing from the Windows local security authority subsystem

Block JavaScript or VBScript from launching downloaded executable content

Block Webshell creation for Servers

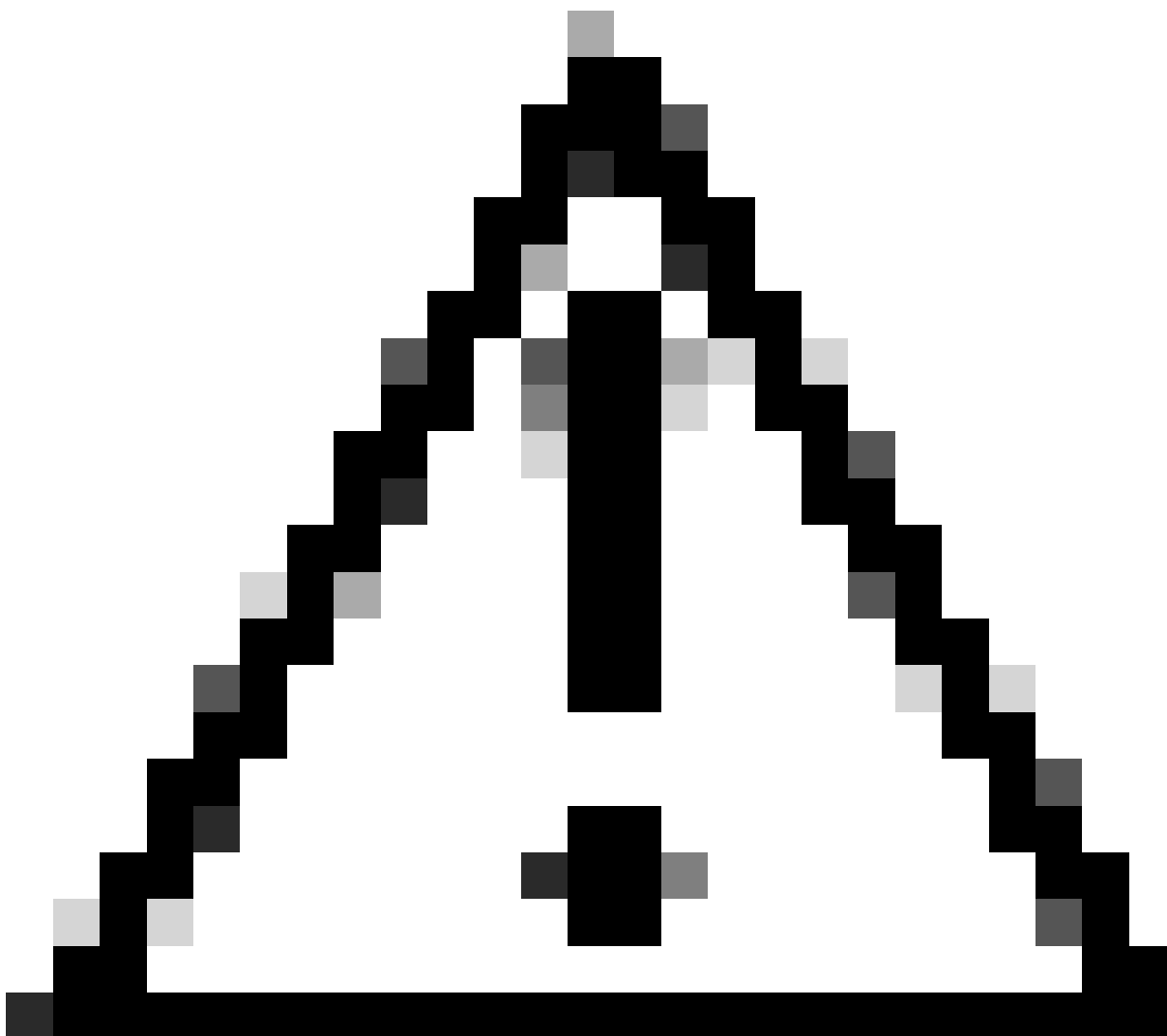
Block trusted and unsigned processes that run from USB

Block persistence through WMI event subscription

**[PREVIEW]** Block use of copied or impersonated system tools

Block abuse of exploited vulnerable signed drivers (Device)

- Home
- Dashboard
- All services
- Devices
- Apps
- Endpoint security
- Reports
- Users
- Groups
- Tenant administration
- Troubleshooting + support



注意：如果遇到此问题，由于缺少sfc.exe，必须启动完全安装

---

## 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）。