# 从思科安全终端中删除过时的Windows例外项

## 目录



## 简介

本文档介绍从Windows安全终端客户环境中删除常见格式错误的排除项的计划过程。

## 问题说明

为了最大限度地降低思科安全终端对性能的影响并最大限度地发挥其功能，我们的工程师已经确定了客户环境中最常见的过时例外项，并将在2022年10月将其删除。安全终端（6.x及更早版本）的早期版本依赖于通配符功能(*)来利用多驱动器例外项。后来对排除定义和输入进行了更改和改进，不再需要这种宽泛的格式，思科维护的排除也进行了调整，以解决通配符创建的性能影响。随着Windows Secure Endpoint 7.5.3的发布，通配符(*)进程排除允许了一项新功能，这改变了星号领先的排除项的处理，并导致在其环境中仍具有以下排除项的客户的cpu消耗增加：

```
*\Windows\Security\database\*.sdb
*\Windows\Security\database\*.edb
*\Windows\Security\database\*.chk
*\Windows\SoftwareDistribution\Datastore\Logs\*.log
*\Windows\Security\database\*.jrs
*\Windows\Security\database\*.log
*\Windows\Temp\content.zip.tmp\*.diff
*\Windows\Temp\content.zip.tmp\cur.scr
*\Windows\Temp\TMP*.tmp
*\Windows\Temp\musdmys_*
*\Windows\Temp\content.zip.tmp\SymDeltaDecompressOptions.xml
*.sas*
*\Windows\SoftwareDistribution\Datastore\Logs\edb*.log
*\System Volume Information\tracking.log
*\Program Files (x86)\SysTrack\LsiAgent\Condense\*\*\*.tmp
*\Program Files (x86)\SysTrack\LsiAgent\Condense\*\*.hld
*\Windows\Temp\AltirisScript*.cmd
*\Windows\System32\drivers\*-*.tmp
*\Users\*\AppData\Local\Temp\*-*.tmp
*\Users\*\AppData\Local\Temp\warsaw_*
*\Windows\Temp\warsaw_*
*Windows\SoftwareDistribution\Datastore\Logs\*.log
*\Windows\System32\Dns\*.dns
*\Windows\System32\DNS\*.scc
*\Windows\ntds\EDB*.log
*\Windows\ntds\Edbres*.jrs
*\Windows\ntds\*.pat
*\Windows\SoftwareDistribution\Datastore\Logs\edb.log
*Windows\Temp\mus*
```

```
*Windows\Temp\content.zip.tmp*
```

# 其他步骤

删除这些排除项不会对环境产生负面影响，并且可提高使用Windows安全终端7.5.3及更高版本的主机的性能。如果您需要多个驱动器，请查看您当前的自定义排除列表，了解任何星号前导(*)排除项，并修改这些排除项，以使用适用于通配符的“应用于所有驱动器号”功能，否则请在路径中提供驱动器号。如果您使用以下任何软件，请确保将思科维护列表添加到策略中，因为已准备好正确的例外项以供使用：

- Microsoft Windows默认值
- 赛门铁克的Altiris
- 域控制器
- 迪博尔德华沙
- Lakeside软件 — Systrack
- SAS应用
- Symantec

  **注意**：如果您的组织内存在与变更冻结相关的顾虑，请最迟在2022年10**月7日打开TAC案例并参考本文。**

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）。